aws

Guida per l'utente

AWS Security Hub



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

AWS Security Hub: Guida per l’utente

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

I marchi e l’immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Cosa sono Security Hub e Security Hub CSPM? 1
AWS Security Hub 2
Funzionalità 2
Integrazioni 3
Accesso al Security Hub 4
Concetti 4
Stimatore dei costi 10
Accesso per tipo di account 11
Prerequisiti 12
Configurazione dell'accesso multi-account 13
Utilizzo dello stimatore dei costi 16
Note importanti 24
Informazioni correlate 24
Abilitazione del Security Hub 24
Abilita Security Hub per un AWS Organizzazione 25
Abilitare Security Hub in un account autonomo 28
Designazione di un amministratore delegato 29
Creazione della politica per gli amministratori delegati 31
Gestione della configurazione degli account dei membri 32
Rimozione di un amministratore delegato 37
Re-enabling Hub di sicurezza 38
Raccomandazioni 38
Copertura dell'account 40
Pagina di copertura dell'account 40
Widget di copertura di sicurezza 42
Piano esteso 42
Autorizzazioni per il piano esteso 43
Iscrizione ai partner del piano esteso 43
Annullamento dell'iscrizione a un partner 44
Cross-Region aggregazione 44
Tipi di dati aggregati 45
Aggregazione per gli account degli amministratori e dei membri 47
Regole di automazione e aggregazione tra regioni 47
Abilitare l'aggregazione 48

Revisione delle impostazioni di aggregazione 48
Aggiornamento delle impostazioni di aggregazione 49
Eliminazione dell'aggregazione 50
Integrazione con Azure 51
Come AWS Config si usa 53
Informazioni aggiuntive 53
Prerequisiti 53
Configurazione di Azure 56
Configurazione di Security Hub 67
Eliminazione di un connettore di Azure 80
Pannello di riepilogo 81
Considerazioni 81
Widget disponibili 82
Filtri disponibili 96
Visualizzazione dei dettagli sulle risorse in Security Hub 97
Formato di ricerca: OCSF 98
Panoramica dell'OCSF 98
Risorse correlate 99
AWS estensione per OCSF 99
Esiti della copertura 122
Risultati della copertura per AWS Security Hub CSPM 122
Risultati della copertura per Amazon GuardDuty 123
Risultati della copertura per Amazon Inspector 123
Risultati della copertura per Amazon Macie 124
Soppressione dei risultati della copertura 124
Inventario AI 125
Prerequisiti per la scoperta dell'IA ospitata autonomamente 125
Tipi di risorse AI supportati 126
Ricerca di risorse AI dalla pagina Risorse 126
Utilizzando la pagina dell'inventario AI 127
Considerazioni 128
Accesso all'inventario AI con l'API 129
Resources 131
In che modo Security Hub individua la criticità 131
Sovrascrivere la criticità con una regola di automazione 131
In che modo la criticità influisce sull'esposizione, individuandone la gravità 131

Risultati dell'esposizione 131
Come funzionano i risultati dell'esposizione 132
Componenti di un rilevamento dell'esposizione 133
Classificazione della gravità 135
Vantaggi dei risultati dell'esposizione 135
Fonti di rilevazione dell'esposizione 135
Best practice 136
Risorse supportate 137
Caratteristiche supportate 138
Generazione di risultati sull'esposizione 141
Determinazione del livello di gravità di un rilevamento dell'esposizione 146
Revisione dei risultati sull'esposizione 148
Grafico del percorso di attacco potenziale 150
Correzione dei risultati dell'esposizione 151
Risultati degli accessi inutilizzati 258
Come funziona l'analisi degli accessi non utilizzati 258
Tipi di ricerca di accesso non utilizzati 259
Service-linked analizzatore 259
Visualizzazione dei risultati di accesso non utilizzati 260
Accesso non utilizzato ai risultati dell'esposizione 260
Raccomandazioni politiche per le autorizzazioni non utilizzate 261
Prezzi 261
Raccomandazioni politiche 261
Come funzionano i consigli sulle policy 261
Chi può generare consigli 262
Ciclo di vita dei consigli 262
Casi di errore 262
Utilizzo della console 263
Guida di riferimento alle API 263
Scansione di rete 263
Tipi di risorse supportati 264
Abilita la scansione di rete 264
Come funziona la scansione in rete 266
Risultati della scansione di rete 266
Scansiona le prove 269
Esclusione delle risorse dalla scansione 270

Porte supportate 270
Multi-cloud supporto 271
Disponibilità nelle regioni 271
Disattiva la scansione di rete 271
Piani di riparazione 272
In che modo Security Hub crea piani di riparazione 272
Dettagli del piano di riparazione 273
Stato del piano di risanamento 273
Linee guida per la riparazione 274
Visualizzazione dei piani di riparazione 275
Filtrare i piani di riparazione 275
Visualizzazione delle esposizioni influenzate da un piano 276
Visualizzazione dei piani di riparazione per un'esposizione 276
Monitoraggio dell'impatto delle misure correttive sulla dashboard 276
Automazioni 276
Regole di automazione 277
EventBridge regole di automazione 301
Esportazione degli esiti 310
Come funziona l'esportazione dei risultati 310
Prerequisiti 310
Creare un'esportazione 311
Third-party integrazioni 3
Jira Cloud 312
ServiceNow 318
Politiche chiave KMS per le integrazioni di ticketing 325
Test delle integrazioni di ticketing 328
App MCP (anteprima) 331
Esempi di app MCP 331
Concetti chiave 335
Prerequisiti 336
Configurazione del server MCP 336
Utilizzo di Connector Diagnostics 337
Strumenti disponibili 338
Monitoraggio dell'utilizzo e dei costi 339
Chi può accedere alla pagina Utilizzo 339
Riepilogo dei costi dell'organizzazione e dell'account 340

Visualizzazione delle capacità ... 341
Visualizzazione dell'account ... 342
Strategie di ottimizzazione dei costi ... 343
Risorse correlate ... 343
Disattivazione di Security Hub ... 343
Disattivazione di Security Hub per un singolo account ... 343
Disattivazione di Security Hub in un'organizzazione ... 344
Sicurezza ... 346
Protezione dei dati ... 347
Gestione dell'identità e degli accessi ... 350
Convalida della conformità ... 383
Resilienza ... 383
Sicurezza dell'infrastruttura ... 383
Endpoint VPC (AWS PrivateLink) ... 384
Registrazione di chiamate API ... 386
Informazioni su Security Hub in CloudTrail ... 386
Esempio: voci del file di registro di Security Hub ... 387
AWS Security Hub CSPM ... 391
Vantaggi del Security Hub CSPM ... 392
Accesso a Security Hub CSPM ... 393
Servizi correlati ... 394
Versione di prova gratuita, utilizzo e prezzi di Security Hub CSPM ... 395
Visualizzazione dei dettagli di utilizzo ... 395
Dettagli prezzi ... 396
Concetti ... 396
Abilitazione del Security Hub CSPM ... 402
Verifica delle autorizzazioni necessarie ... 402
Abilitazione di Security Hub CSPM con l'integrazione delle organizzazioni ... 402
Abilitazione manuale di Security Hub CSPM ... 405
Passaggi successivi: gestione e integrazioni della postura ... 407
Configurazione AWS Config ... 407
Configurazione locale ... 414
Configurazione centrale ... 415
Gestione di più account ... 464
Gestione degli account conAWS Organizations ... 464
Gestione manuale degli account tramite invito ... 465

Consigli per ambienti con più account 466
Gestione degli account con AWS Organizations 468
Gestione degli account tramite invito 484
Azioni consentite dagli account degli amministratori e dei membri 498
Effetto delle azioni dell'account sui dati 505
Aggregazione dei dati tra le regioni 507
Tipi di dati aggregati 509
Aggregazione per gli account degli amministratori e dei membri 510
Configurazione e aggregazione centralizzate 511
Abilitare l'aggregazione 512
Revisione delle impostazioni di aggregazione 514
Aggiornamento delle impostazioni di aggregazione 516
Interruzione dell'aggregazione 518
Standard 519
Riferimento agli standard 521
Abilitazione di uno standard 633
Revisione dei dettagli di uno standard 640
Disattivazione degli standard con attivazione automatica 643
Disabilitazione di uno standard 645
Controlli 648
Visualizzazione consolidata dei controlli 648
Punteggio di sicurezza riepilogativo per i controlli 649
Riferimento ai controlli 650
Autorizzazioni per configurare i controlli 1577
Abilitazione dei controlli 1578
Disattivazione dei controlli 1587
Controlli e punteggi di sicurezza 1598
Categorie di controllo 1675
Revisione dei dettagli dei controlli 1679
Filtraggio e ordinamento dei controlli 1682
Parametri di controllo 1683
Revisione e gestione dei risultati del controllo 1697
Integrazioni 1726
Revisione di un elenco di integrazioni 1727
Abilitare il flusso dei risultati derivanti da un'integrazione 1728
Disattivazione del flusso di risultati da un'integrazione 1730

Visualizzazione dei risultati di un'integrazione 1731
Servizio AWS integrazioni 1731
Third-party integrazioni 1753
Integrazioni di prodotti personalizzate 1788
Integrazione con Azure 1791
Come AWS Config viene usato 1792
tipi di connettori 1792
Prerequisiti 1793
Configurazione di Azure 1796
Configurazione del Security Hub CSPM 1802
Eliminazione di un connettore Azure 1826
Esiti 1827
BatchImportFindings per trovare fornitori 1829
BatchUpdateFindings per i clienti 1832
Revisione dei dettagli e della cronologia dei risultati 1836
Filtro dei risultati 1841
Raggruppamento degli esiti 1843
Impostazione dello stato dei risultati del flusso di lavoro 1844
Invio dei risultati a un'operazione personalizzata 1847
Formato di ricerca: ASFF 1848
Approfondimenti 2145
Revisione e azione in base agli approfondimenti 2146
Informazioni dettagliate gestite 2149
Informazioni personalizzate 2160
Automazioni 2168
Regole di automazione 2169
Risposta e riparazione automatiche 2195
Pannello di riepilogo 2211
Widget disponibili per la dashboard di riepilogo 2212
Filtraggio del pannello di controllo 2216
Personalizzazione della dashboard 2218
Limiti regionali 2219
Cross-Region restrizioni di aggregazione 2219
Disponibilità di integrazioni per regione 2219
Disponibilità degli standard per regione 2222
Disponibilità dei controlli per regione 2222

Limiti regionali sui controlli 2222
Creazione di risorse con CloudFormation 2492
Security Hub CSPM eCloudFormationmodelli 2493
Scopri di più suCloudFormation 2493
Iscrizione agli annunci 2494
Formato dei messaggi Amazon SNS 2499
Disattivazione del Security Hub CSPM 2501
Sicurezza 2503
Protezione dei dati 2504
Gestione dell'identità e degli accessi 2505
Convalida della conformità 2540
Resilienza 2541
Sicurezza dell'infrastruttura 2541
Endpoint VPC (AWS PrivateLink) 2542
Registrazione di chiamate API 2543
Informazioni CSPM di Security Hub in CloudTrail 386
Esempio: voci del file di registro CSPM di Security Hub 387
Applicazione di tag alle risorse 2547
Nozioni fondamentali sull'etichettatura 2547
Utilizzo di tag nelle policy IAM 2549
Aggiunta di tag alle risorse 2550
Modifica dei tag per le risorse 2552
Revisione dei tag per le risorse 2554
Rimozione dei tag dalle risorse 2557
Quote 2559
Quote massime 2559
Quote tariffa 2559
Cronologia dei documenti 2560
..... mmdclxxx

Cosa sono Security Hub e Security Hub CSPM?

AWSSecurity Hub e AWS Security Hub CSPM Servizi AWS proteggono il tuo ambiente cloud. I servizi si completano a vicenda. Se utilizzati insieme, forniscono informazioni preziose sul livello di sicurezza dell'AWSambiente.

Security Hub CSPM offre una visione completa del tuo livello di sicurezza e ti aiuta a valutare il tuo ambiente cloud rispetto agli standard e alle best practice del settore della sicurezza. Security Hub offre un'esperienza unificata che ti aiuta a stabilire le priorità e a rispondere ai problemi di sicurezza critici. I risultati CSPM di Security Hub vengono indirizzati automaticamente a Security Hub, dove vengono correlati ai risultati di altri servizi di sicurezza, come Amazon Inspector, per generare esposizioni. Questo ti aiuta a identificare i rischi più critici nel tuo ambiente. Security Hub offre anche funzionalità di flusso di lavoro automatizzate, che consentono di incorporare i risultati CSPM di Security Hub nei flussi di lavoro operativi.

Come best practice, consigliamo di abilitare entrambi i servizi. Puoi abilitare Security Hub CSPM senza abilitare Security Hub se il tuo obiettivo principale è identificare configurazioni errate e valutare il tuo livello di sicurezza. Tuttavia, se si abilita Security Hub senza abilitare Security Hub CSPM, Security Hub non può utilizzare i risultati CSPM di Security Hub per fornire informazioni sui rischi e le esposizioni nel proprio ambiente. AWS Per un'esperienza ottimale, consigliamo non solo di abilitare Security Hub e Security Hub CSPM, ma anche di abilitare questi altri servizi di sicurezza: Amazon GuardDuty, AmazonInspector e Amazon Macie.

Introduzione a AWS Security Hub

AWS Security Hub è una soluzione di sicurezza cloud unificata che dà priorità ai problemi di sicurezza critici e ti aiuta a rispondere su larga scala. Security Hub rileva i problemi di sicurezza correlando e arricchendo automaticamente i segnali di sicurezza provenienti da più fonti. Queste fonti includono la gestione della postura, la gestione delle vulnerabilità (Amazon Inspector), i dati sensibili (Amazon Macie) e il rilevamento delle minacce (Amazon). GuardDuty Usa Security Hub per dare priorità ai rischi attivi nel tuo ambiente cloud attraverso analisi automatizzate e approfondimenti contestuali. Attraverso visualizzazioni intuitive, Security Hub trasforma segnali di sicurezza complessi in informazioni fruibili, che consentono di prendere decisioni informate sulla sicurezza in modo rapido. Security Hub include anche flussi di lavoro di risposta automatizzati per aiutarti a correggere i rischi, migliorare la produttività del team e ridurre al minimo le interruzioni operative.

Funzionalità

Soluzione di sicurezza unificata

Ottieni una maggiore visibilità sul tuo ambiente cloud attraverso la gestione centralizzata in una soluzione di sicurezza cloud unificata.

Informazioni sulla sicurezza utilizzabili

Ottieni informazioni utili sulla sicurezza attraverso analisi avanzate per conoscere i rischi per la sicurezza associati al tuo ambiente.

Tempi di risposta ridotti

Semplifica i tempi di risposta con flussi di lavoro automatizzati e un sistema di ticketing integrato.

Risultati dell'esposizione

Security Hub mette in correlazione i risultati dei controlli di controllo CSPM di Security Hub, Amazon Inspector e altro Servizi AWS per rilevare le esposizioni associate alle risorse. AWS

Analisi degli accessi non utilizzati

Security Hub identifica automaticamente i ruoli, gli utenti, le chiavi di accesso e le autorizzazioni IAM che non sono stati utilizzati entro un periodo di lookback di 90 giorni. Quando abiliti Security

Hub, il servizio crea un IAM Access Analyzer collegato al servizio nel tuo account. I risultati sugli accessi non utilizzati aiutano a implementare l'accesso con privilegi minimi evidenziando i principi IAM sovraassegnati. Per quanto riguarda i risultati delle autorizzazioni non utilizzate, Security Hub può generare raccomandazioni sulla politica dei privilegi minimi che mostrano una politica sostitutiva mirata.

I risultati sono formattati nell'Open Cybersecurity Schema Framework (OCSF)

Security Hub genera risultati in OCSF e riceve risultati in OCSF da Security Hub CSPM e altri: Servizi AWS

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

Pannello di controllo

La console Security Hub offre una visione completa delle esposizioni, delle minacce, della copertura di sicurezza e delle risorse, oltre a una visualizzazione interattiva chiamata grafico del percorso di attacco, che mostra come i potenziali aggressori possono accedere e assumere il controllo delle risorse associate a un rilevamento dell'esposizione.

Integrazioni con prodotti di terze parti

Puoi migliorare il tuo livello di sicurezza con le integrazioni di Security Hub. Ad esempio, se utilizzi Jira Cloud oServiceNow ITSM, puoi utilizzare questa funzione per creare ticket a partire dai risultati.

Integrazioni

Security Hub riceve i risultati da quanto segue Servizi AWS.

- AWS Security Hub CSPM
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- Sistema di analisi degli accessi IAM

Accesso al Security Hub

Security Hub è disponibile nella maggior parte AWS delle regioni. Per un elenco delle regioni in cui Security Hub è attualmente disponibile, consulta Endpoint e quote del Security Hub nel. Riferimenti generali di AWS Per informazioni sulla gestione Regioni AWS del tuo account Account AWS, consulta Specificare quale Regioni AWS account può utilizzare nella Gestione dell'account AWS Guida di riferimento.

Puoi abilitare Security Hub per singoli account o account della tua organizzazione. In ogni regione, puoi accedere e utilizzare Security Hub in uno dei seguenti modi:

Console Security Hub

La console Security Hub è un'interfaccia basata su browser che puoi utilizzare per creare e gestire AWS risorse. In questa console puoi accedere al tuo account, ai dati e alle risorse.

API Security Hub

L'API Security Hub ti offre l'accesso programmatico al tuo account, ai dati e alle risorse. Puoi inviare richieste HTTPS direttamente a Security Hub.

AWS CLI

Con AWS CLI, è possibile eseguire comandi nella riga di comando del sistema per eseguire attività e creare script che eseguano attività. In alcuni casi, AWS CLI può essere più utile della console Security Hub.

AWS SDK

AWS Gli SDK sono costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione (C++, Go, Java, .NET e Python). Forniscono l'accesso programmatico a Security Hub e ad altro Servizi AWS nella lingua preferita e possono aiutarti a gestire attività come la gestione degli errori, la firma delle richieste e il ritentativo delle richieste.

Concetti relativi al Security Hub

In Security Hub, ci basiamo su AWS concetti e terminologia comuni e utilizziamo questi termini aggiuntivi.

Account

L' AWS account standard contenente AWS le tue risorse. Accedi AWS con il tuo AWS account per abilitare Security Hub.

Se l'account è registrato AWS Organizations, l'organizzazione designa un account amministratore di Security Hub. Questo account può abilitare altri account dell'organizzazione come account membro.

Un'organizzazione può avere un solo account amministratore. Un account non può essere contemporaneamente un account amministratore e un account membro.

Security Hub supporta i seguenti account:

- Account di gestione dell'organizzazione: un AWS account che amministra un' AWS organizzazione.
- Account amministratore delegato: un AWS account che gestisce l'uso di un account Servizio AWS per un' AWS organizzazione.
- Account membro: un AWS account membro di un' AWS organizzazione.
- Account autonomo: un AWS account non AWS Organizations abilitato.

Account amministratore

Questo tipo di AWS account può visualizzare i risultati degli account dei membri associati.

Questo tipo di AWS account diventa un account amministratore quando l'account viene designato da un account di gestione dell'organizzazione come account amministratore del Security Hub. L'account amministratore di Security Hub può abilitare qualsiasi account dell'organizzazione come account membro e può anche invitare altri account a diventare account membro.

Un'organizzazione può avere un solo account amministratore. Un account non può essere contemporaneamente un account amministratore e un account membro.

Regione di aggregazione

Una regione di aggregazione consente di visualizzare i risultati di sicurezza provenienti da più parti Regioni AWS in un unico pannello di controllo.

La regione di aggregazione è l'area Regione AWS in cui è possibile visualizzare e gestire i risultati. I risultati vengono aggregati nella regione di aggregazione delle regioni collegate. I risultati aggiornati vengono replicati in tutte le regioni.

Nella regione di aggregazione, la dashboard e le pagine di inventario includono i dati di tutte le regioni collegate. La pagina delle automazioni può essere utilizzata solo per definire le regole di automazione nell'area di aggregazione. Third-party le integrazioni di ticketing possono essere configurate solo nella regione di aggregazione.

Risultati archiviati

Un risultato con uno stato di. `ARCHIVED` Questi risultati indicano che il fornitore o il cliente che esamina il risultato ritiene che il risultato non sia più pertinente.

I fornitori di servizi di ricerca possono archiviare i risultati che creano. I clienti possono archiviare tutti i risultati che ritengono non più pertinenti utilizzando BatchUpdateFindingsV2l'API Security Hub o aggiornando lo stato nella console Security Hub.

Nella console Security Hub, le impostazioni di filtro predefinite escludono i risultati archiviati dagli elenchi e dalle tabelle dei risultati. È possibile aggiornare i filtri per includere i risultati archiviati. Se si recuperano i risultati utilizzando l'operazione GetFindingsV2, l'operazione recupera sia i risultati archiviati che quelli attivi. L'esempio seguente mostra come escludere i risultati archiviati nei risultati.

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

Cross-Region aggregazione

L'aggregazione dei risultati e delle risorse provenienti dalle regioni collegate a una regione di aggregazione. Puoi visualizzare tutti i dati della regione di aggregazione e aggiornare i risultati della regione di aggregazione.

Account amministratore delegato

In AWS Organizations, l'account amministratore delegato per un servizio è in grado di gestire l'uso di un servizio per l'organizzazione.

In Security Hub, l'account amministratore di Security Hub è anche l'account amministratore delegato per Security Hub. Quando l'account di gestione dell'organizzazione designa per la prima volta l'account amministratore di Security Hub, Security Hub chiama Organizations per rendere quell'account l'account amministratore delegato.

L'account di gestione dell'organizzazione deve quindi scegliere l'account amministratore delegato come account amministratore di Security Hub in tutte le regioni.

Exposure

Le esposizioni sono punti deboli più ampi nei controlli di sicurezza, configurazioni errate o altre aree che potrebbero essere sfruttate da minacce attive.

Esempi di esposizioni includono:

- Piano di controllo configurato in modo errato per una risorsa.
- Presenza di una vulnerabilità del software con un elevato potenziale di sfruttabilità.
- Risorsa accessibile al pubblico (rete o API).

Rilevamento dell'esposizione

Un tipo di risultato che descrive un'esposizione presente nell'ambiente. Un risultato sull'esposizione include caratteristiche e segnali. Un segnale può includere uno o più tipi di caratteristiche di esposizione. AWS Security Hub genera un risultato di esposizione quando i segnali provenienti da AWS Security Hub CSPM, Amazon Inspector, GuardDuty Amazon, Amazon Macie AWS o altri servizi indicano la presenza di un'esposizione. Una risorsa può essere coinvolta in uno o più risultati sull'esposizione. Se una risorsa non presenta caratteristiche di esposizione o presenta caratteristiche insufficienti, Security Hub non genera un risultato di esposizione per quella risorsa.

Un esempio di rilevamento dell'esposizione è: un'istanza EC2 raggiungibile da Internet e che presenta vulnerabilità software che hanno un'alta probabilità di sfruttamento.

Risultato

La registrazione osservabile di un controllo di sicurezza o di un rilevamento correlato alla sicurezza. Security Hub genera e aggiorna i risultati attraverso la correlazione di altri risultati di

sicurezza. Questi sono chiamati risultati sull'esposizione. I risultati possono provenire anche da integrazioni con altri prodotti Servizi AWS e di terze parti.

Individuazione dell'ingestione

L'importazione dei risultati in Security Hub. Gli eventi di ingestione di Finding includono sia nuovi risultati che aggiornamenti dei risultati esistenti.

Regione collegata

Quando si abilita l'aggregazione tra aree geografiche, una regione collegata è un'area che aggrega i risultati e l'inventario delle risorse nella regione di aggregazione.

In una regione collegata, la dashboard e le pagine di inventario contengono solo i risultati relativi a tale area. Regione AWS

Framework di schemi di sicurezza informatica aperto (OCSF)

L'Open Cybersecurity Schema Framework (OCSF) è uno sforzo collaborativo e open source di partner leader nel settore della sicurezza informatica. AWS OCSF fornisce uno schema standard per gli eventi di sicurezza più comuni, definisce i criteri di controllo delle versioni per facilitare l'evoluzione dello schema e include un processo di autogoverno per produttori e consumatori di registri di sicurezza. Per ulteriori informazioni, consulta i risultati OCSF in Security Hub.

Account membro

E Account AWS che ha concesso l'autorizzazione a un account amministratore di visualizzare i risultati e intervenire in base a tali risultati. Questo tipo di account Account AWS diventa membro quando l'account amministratore di Security Hub lo abilita come account membro.

Signal

Una scoperta che contribuisce a un accertamento dell'esposizione. Un segnale può essere definito un risultato che contribuisce. Un segnale può avere origine in Security Hub CSPM o altro AWS Config Servizi AWS, come Amazon Inspector.

Service-linked registratore di configurazione

Un tipo di AWS Config registratore utilizzato per registrare i dati di configurazione su risorse specifiche del servizio. Security Hub utilizza questi registratori in un approccio basato sugli eventi per ottenere elementi di configurazione delle risorse per la copertura dell'analisi dell'esposizione, la rendicontazione dell'inventario delle risorse e le valutazioni del controllo della gestione della postura. Questa funzionalità viene fornita a tutti i clienti Security Hub come parte dei prezzi del piano Essential. Dopo aver abilitato Security Hub, nel tuo account vengono creati i seguenti registratori di configurazione collegati ai servizi:

- In ogni lato Regione AWS, viene Account AWS creato un registratore di configurazione collegato al servizio denominato. `AWSConfigurationRecorderForSecurityHubAssets`
- Per i tipi di risorse globali, `AWSConfigurationRecorderForSecurityHubAssetsGlobal` viene creato un registratore di configurazione aggiuntivo collegato ai servizi denominato us-east-1. Regione AWS
- Se Security Hub e Security Hub CSPM sono entrambi abilitati in un Account AWS e Regione AWS, viene creato un registratore di configurazione collegato al servizio denominato. `AWSConfigurationRecorderForSecurityHubCSPM`

Per ulteriori informazioni, vedere Considerazioni per i registratori di configurazione collegati ai servizi e Registrazione delle risorse regionali e globali.

Service-linked analizzatore

Un IAM Access Analyzer che Security Hub crea e gestisce per tuo conto. Quando abiliti Security Hub, crea automaticamente un analizzatore di accessi inutilizzati collegato al servizio per identificare i ruoli, gli utenti, le chiavi di accesso e le autorizzazioni IAM che non sono stati utilizzati entro un periodo di lookback di 90 giorni. L'analizzatore viene eseguito negli Stati Uniti orientali (Virginia settentrionale) perché IAM è un servizio globale. Security Hub replica i risultati di accesso non utilizzati in tutte le regioni in cui è stato abilitato Security Hub. Non è necessario abilitare separatamente IAM Access Analyzer o intraprendere alcuna azione aggiuntiva. Questa funzionalità viene fornita a tutti i clienti Security Hub come parte dei prezzi del piano Essential. È possibile visualizzare l'analizzatore collegato al servizio nella console IAM Access Analyzer, ma non è possibile modificarlo o eliminarlo mentre Security Hub è abilitato. Security Hub elimina l'analizzatore quando si disabilita il servizio in tutte le regioni di un. Account AWS Per ulteriori informazioni, consulta the section called "Risultati degli accessi inutilizzati".

Tratto

Una deviazione di sicurezza che dà come risultato un rilevamento dell'esposizione. I tipi di caratteristiche includono presupponibilità, errata configurazione, raggiungibilità, dati sensibili e vulnerabilità. Una caratteristica è associata a un segnale e un segnale può contenere più caratteristiche. Ad esempio, un controllo CSPM di Security Hub indica che una politica gestita dal cliente consente il controllo amministrativo degli accessi. Questo segnale contiene una caratteristica di configurazione errata.

Risultati degli accessi inutilizzati

Un risultato che identifica un ruolo, un utente, una chiave di accesso o un set di autorizzazioni IAM che non sono stati utilizzati entro un periodo di lookback di 90 giorni. Security Hub genera risultati

di accesso non utilizzati utilizzando un IAM Access Analyzer collegato al servizio. Esistono quattro tipi di risultati di accesso non utilizzati: ruoli IAM non utilizzati, chiavi di accesso utente IAM non utilizzate, password utente IAM non utilizzate e autorizzazioni non utilizzate.

AWS Stima dei costi di Security Hub

Lo stimatore dei costi di Security Hub è una funzionalità della console che fornisce stime delle funzionalità di Security Hub in tutto l' AWS ambiente. Lo strumento di stima dei costi mostra quali sono i costi dei singoli servizi tra AWS Security Hub CSPM, Amazon Inspector e Amazon GuardDuty e quali sarebbero i costi stimati in Security Hub con i piani tariffari semplificati di Security Hub. Puoi modificare l'utilizzo stimato e il conteggio delle risorse in modo che corrispondano al tuo AWS utilizzo per aumentare la precisione della stima. Lo strumento di stima dei costi è disponibile in tutte le regioni in cui Security Hub è disponibile.

Lo stimatore dei costi stima i costi mensili per le funzionalità di sicurezza utilizzando due modelli di prezzo:

- Prezzi dei singoli servizi: paga separatamente ciascuna funzionalità di sicurezza (Amazon InspectorGuardDuty, Security Hub CSPM).
- Prezzi semplificati di Security Hub: prezzi unificati su 3 piani tariffari, piano Essentials con prezzi per risorsa, analisi delle minacce con prezzi per evento e per GB di log e scansione del codice Lambda con prezzi per risorsa.

AWS Cost Explorer Lo stimatore utilizza i dati quando disponibili. Quando i dati di Cost Explorer non sono disponibili, è possibile inserire manualmente i dati di utilizzo. Le stime dei costi si basano sull'utilizzo osservato e fornito dall'utente e sulle informazioni pubbliche sui prezzi. Le stime potrebbero non riflettere gli sconti aziendali.

I principali vantaggi dello strumento di stima dei costi includono:

- Scopri come il costo con prezzi unificati, quando abiliti Security Hub, si confronta con il costo del singolo servizio senza abilitare Security Hub
- Stima i costi prima di abilitare le funzionalità
- Modifica i parametri di utilizzo per modellare diversi scenari
- Esporta le stime in formato PDF per la revisione da parte delle parti interessate

Accesso per tipo di account

> **Note**
>
> Per gli account amministratori e membri delegati, lo strumento di stima dei costi si apre in modalità di modifica per impostazione predefinita, consentendo di inserire immediatamente i dati di utilizzo. L'account di gestione e gli account autonomi si aprono in modalità di visualizzazione quando i dati di Cost Explorer sono disponibili.

Questa funzione recupera automaticamente le informazioni sull'effettivo utilizzo passato per stimare il costo per determinati tipi di account. Consulta la tabella seguente per i dettagli su ciascun tipo di account e i dati disponibili per ciascun tipo di account.

Autorizzazioni di accesso per tipo di account

Tipo di account	Dati di Cost Explorer	Inserimento dati	Scope
Account di gestione (MA)	Auto-populated	Sostituzione manuale disponibile	Organization-wide
Amministratore delegato (DA)	Auto-populated tramite il ruolo di più account*	È disponibile l'override manuale	Organization-wide
Member Account	Auto-populated tramite un ruolo su più conti*	È disponibile l'override manuale	Organization-wide
Account autonomo (SA)	Auto-populated	Sostituzione manuale disponibile	Account singolo

* Richiede la configurazione del ruolo IAM per più account nell'account di gestione. Vedi la Configurazione dell'accesso multi-account sezione seguente.

Prerequisiti

Autorizzazioni IAM richieste

Per utilizzare tutte le funzionalità dello strumento di stima dei costi, il responsabile IAM deve disporre delle seguenti autorizzazioni:

Autorizzazioni IAM richieste per Cost Estimator

Operazione API	Servizio	Scopo
`ce:GetCostAndUsage`	AWS Cost Explorer	Recupera i dati storici sull'utilizzo e sui costi
`pricing:GetProducts`	AWS Prezzi	Ottieni le tariffe attuali
`organizations:ListAccounts`	AWS Organizzazioni	Conta gli account nell'organizzazione
`organizations:DescribeOrganization`	AWS Organizzazioni	Determina il tipo di account
`securityhub:ListOrganizationAdminAccounts`	Hub di sicurezza	Elenca gli account amministrativi dell'organizzazione
`iam:GetRole`	IAM	Verifica l'esistenza del ruolo tra più account (solo account di gestione) *
`sts:AssumeRole`	IAM	Assumi un ruolo con più account (solo administrator/Member account delegato) **

* Richiesto solo per gli utenti dell'account di gestione per verificare lo stato del ruolo tra account.

** Richiesto solo per gli account Amministratore delegato e Membro dell'organizzazione che utilizzano l'accesso tra più account.

Requisiti aggiuntivi

Esploratore dei costi

Deve essere abilitato per la compilazione automatica dei dati (ritardo di elaborazione di 24 ore dopo l'abilitazione).

Configurazione dell'accesso multi-account

Gli account amministratori e membri delegati possono accedere ai AWS Cost Explorer dati a livello di organizzazione dall'account di gestione configurando un ruolo IAM tra account. Questa configurazione consente a questi account di visualizzare i dati di utilizzo effettivi senza passare all'account di gestione.

Prerequisiti

I seguenti elementi e informazioni sono necessari prima di configurare l'accesso tra più account per lo stimatore dei costi:

- L'account di gestione deve essere abilitato AWS Cost Explorer .
- Autorizzazioni IAM per creare ruoli nell'account di gestione.
- Conoscenza dell'ID dell'amministratore delegato o dell'account membro a cui verrà concesso l'accesso tra più account.

Passaggi di impostazione

Lo strumento di stima dei costi fornisce istruzioni di configurazione guidate direttamente nella console. Per accedere alle istruzioni, accedi alla pagina dello strumento di stima dei costi all'indirizzo https://console.aws.amazon.com/securityhub/v2/home #/CostEstimator nell'account di gestione dell'organizzazione. Individua la sezione di Cross-account accesso e segui i passaggi descritti per configurare il ruolo tra account.

Configurazione del ruolo

L'accesso tra account per lo stimatore dei costi richiede l'impostazione di un ruolo IAM con una politica di fiducia e una politica di autorizzazioni. Il ruolo tra account deve essere creato nell'account di gestione con la seguente configurazione:

Nome del ruolo (nome esatto richiesto) — AwsSecurityHubCostEstimatorCrossAccountRole

Politica di fiducia consigliata:

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

Modifica la policy sostituendo i seguenti valori nell'esempio di policy:

- Sostituiscilo *{ACCOUNT_ID}* con l'ID dell'amministratore delegato o dell'account membro a cui stai concedendo l'accesso tra più account.
- Sostituiscilo *{ROLE_NAME}* con il nome del ruolo IAM nell'account amministratore o membro delegato a cui stai concedendo l'accesso.

Politica delle autorizzazioni consigliata:

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

> **Note**
>
> La politica di fiducia limita l'accesso a un account e a un ruolo specifici. Solo il responsabile IAM specificato può assumere questo ruolo, impedendo accessi non autorizzati.

Verifica

Dopo aver creato il ruolo nell'account di gestione, segui i passaggi seguenti per confermare che la configurazione funziona.

1. Accedi all'account amministratore o membro delegato.
2. Accedi allo strumento di stima dei costi di Security Hub all'indirizzo #/CostEstimator https://console.aws.amazon.com/securityhub/v2/home
3. La pagina dovrebbe automaticamente:
    a. Rileva l'account di gestione nella tua organizzazione.
    b. Assumi il ruolo di più account.
    c. Carica i dati di Cost Explorer utilizzandoli a livello di organizzazione.

In caso di successo, vengono visualizzati i dati di utilizzo effettivo anziché i campi di immissione manuale.

Risoluzione dei problemi

Questa sezione illustra i problemi e le soluzioni comuni che possono verificarsi durante la configurazione dell'accesso tra account.

I dati di utilizzo organizzativi non sono disponibili per questo account

Questo avviso indica che il ruolo tra account non è accessibile. Le possibili cause di questo avviso sono:

1. Il ruolo non esiste: l'account di gestione non ha ancora creato il ruolo.
    - Soluzione: contattate l'amministratore dell'account di gestione per creare il ruolo utilizzando la guida alla configurazione.
2. Mancata corrispondenza del nome del ruolo: il nome del ruolo non corrisponde esattamente.

- Soluzione: verificare che il nome del ruolo sia`AwsSecurityHubCostEstimatorCrossAccountRole`.

3. Politica di fiducia errata: la politica di fiducia non consente all'account di assumere il ruolo.
   - Soluzione: verifica che la politica di fiducia includa l'ID dell'account e il nome del ruolo.
4. AssumeRole Autorizzazione mancante: il tuo responsabile IAM non funziona`sts:AssumeRole`.
   - Soluzione: contatta il tuo amministratore per aggiungere `sts:AssumeRole` l'autorizzazione.

Per visualizzare istruzioni di configurazione dettagliate: scegli Visualizza istruzioni nell'avviso per aprire una finestra modale con linee guida dettagliate e modelli di policy.

Soluzione alternativa: puoi comunque utilizzare il Cost Estimator inserendo manualmente i valori di utilizzo in modalità di modifica.

Utilizzo dello stimatore dei costi

Accesso allo stimatore dei costi

Per accedere al Cost Estimator dalla landing page di Security Hub

1. Accedi al tuo AWS account con le credenziali dell'account di gestione AWS dell'organizzazione o di amministratore delegato. Apri la console Security Hub nella regione us-east-1 all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
2. Nella pagina di destinazione, individua la scheda dei prezzi.
3. Scegli Costo stimato.

Per accedere al Cost Estimator durante le fasi di attivazione e configurazione di Security Hub

1. Individua i prezzi nella nuova scheda Security Hub nell'interfaccia di onboarding.
2. Scegli Visualizza stime.

Per accedere allo strumento di stima dei costi dalle console GuardDuty Amazon Inspector o Security Hub CSPM

1. Accedi al pannello di controllo o alla pagina di riepilogo del servizio.

2. Scegli Confronta prezzi nella scheda informativa sui prezzi.

Comprendere l'interfaccia dello strumento di stima dei costi

Layout della pagina

La pagina Cost Estimator contiene tre sezioni principali:

- Sezione panoramica: illustra i vantaggi della gestione unificata della sicurezza e dell'ottimizzazione dei costi.
- Informazioni sui prezzi: pannello espandibile con categorie di funzionalità e livelli di prezzo.
- Tabella di confronto dei prezzi: confronto Side-by-side dei costi con dettagli sulle capacità.

Tabella di confronto dei prezzi

L'intestazione della tabella include i controlli di view/edit modalità e un'opzione di ripristino. La tabella mostra i costi in due colonne:

- Servizi singoli: costi attuali o stimati per servizi di sicurezza separati.
- Security Hub: costi stimati utilizzando un modello di prezzo semplificato.

Regione tariffaria

La prima colonna mostra le informazioni sul contesto dei prezzi, inclusa una nota secondo cui le stime utilizzano i prezzi us-east-1 per i calcoli. Un badge indica che gli sconti aziendali non sono inclusi nelle stime.

Visualizzazione delle stime dei costi

Quando si utilizza lo stimatore dei costi è possibile visualizzare, modificare, reimpostare ed esportare le stime.

Per impostazione predefinita, lo strumento di stima dei costi si apre in modalità di visualizzazione.

Per visualizzare le stime dei costi

1. Accedere al Cost Estimator utilizzando uno dei metodi descritti inAccesso allo stimatore dei costi.
2. Rivedi i costi mensili totali nella riga di riepilogo.

3. Esamina i gruppi di capacità e la loro ripartizione dettagliata dei costi.
4. Scegli i nomi delle funzionalità per visualizzare le descrizioni in un popover.

Origini dati in modalità di visualizzazione

Lo stimatore visualizza i dati provenienti da più fonti, indicati da etichette:

- Predefinito: dati di AWS Cost Explorer (ultimi 30 giorni).
- $-/mo: dati sui costi non disponibili (visualizzati quando l'accesso a Cost Explorer non è disponibile).
- Utilizzo personalizzato: valori. User-entered
- Non abilitato: mostra quando le autorizzazioni di Cost Explorer non esistono.

Account-specific comportamento

Di seguito viene descritto come funziona lo stimatore dei costi su diversi tipi di account e configurazioni.

Account per amministratori e membri delegati

Con l'accesso tra più account configurato:

- I dati di Cost Explorer sono disponibili per l'utilizzo a livello di organizzazione.
- Si apre in modalità di visualizzazione per impostazione predefinita (uguale all'account di gestione). È possibile passare alla modalità di modifica per modificare le stime.

Senza l'accesso tra più account configurato:

- Viene visualizzato l'avviso: «I dati di utilizzo dell'organizzazione non sono disponibili per questo account».
- Per impostazione predefinita, si apre in modalità di modifica per l'immissione manuale.
- Scegli Visualizza istruzioni nell'avviso per una guida alla configurazione.

Gestione dell'account

Con il ruolo tra più account creato:

- La sezione "Cross-account access» mostra lo stato configurato.
- Visualizza le politiche consigliate per la verifica.
- Fornisce un collegamento per visualizzare il ruolo nella console IAM.

Senza la creazione di un ruolo tra più account:

- la sezione "Cross-account access» mostra la guida alla configurazione.
- Fornisce istruzioni dettagliate con politiche precompilate.
- Collegamento diretto alla console IAM per la creazione dei ruoli.

Impossibile verificare lo stato del ruolo:

- Se non si dispone dell'autorizzazione per la chiamata`iam:GetRole`, la console non è in grado di determinare se è stato creato il ruolo necessario.
- Mostra «Impossibile verificare» con il messaggio di errore corrispondente.

Account autonomo

Senza la creazione di un ruolo tra più account:

- Nessuna modifica al comportamento esistente.
- I dati di Cost Explorer sono disponibili se abilitati.
- Per impostazione predefinita, si apre in modalità di visualizzazione.

Modifica dei valori di utilizzo

La modalità di modifica consente di modificare i valori delle dimensioni e visualizzare gli aggiornamenti dei costi in tempo reale.

Per modificare i valori di utilizzo

1. Scegli Modifica nell'intestazione della tabella.
2. Immettete i valori nei campi di immissione delle dimensioni.
3. Visualizza automaticamente i costi aggiornati.
4. Scegli Visualizza per tornare alla modalità di visualizzazione.

Important

- Le modifiche non vengono salvate quando si esce dalla pagina di stima dei costi
- Le stime modificate utilizzano i prezzi us-east-1 (Virginia settentrionale) e non includono sconti aziendali
- La modifica in modalità «Mostra solo il costo corrente» torna automaticamente alla modalità stimata

Reimpostazione dello stimatore

Questa azione cancella tutti i valori personalizzati e ricarica i dati predefiniti da Cost Explorer.

Per ripristinare tutti i valori predefiniti

1. Scegli Reimposta nell'intestazione della tabella.
2. Nella finestra di dialogo di conferma, scegli Reimposta.

Esportazione delle stime

Mentre sei nello strumento di stima dei costi, i dati della stima possono essere esportati in un file PDF.

Per esportare le stime dei costi

1. Assicurati di essere in modalità di visualizzazione.
2. Scegli Scarica PDF nell'intestazione della pagina.

Il PDF viene scaricato automaticamente con il nome del file:. `SecurityHub-Cost-Estimate-YYYY-MM-DD.pdf`

Risoluzione dei problemi

Questa sezione descrive i problemi e le soluzioni comuni che possono verificarsi quando si utilizza lo stimatore dei costi

Nessun dato di Cost Explorer disponibile

Problema

L'avviso mostra «Nessun dato sui costi disponibile per il tuo account».

Soluzioni per tipo di account

La soluzione dipende dal tipo di account:

Soluzioni per i dati mancanti di Cost Explorer

Tipo di account	Soluzione
Account di gestione	Abilita Cost Explorer e attendi 24 ore per l'elaborazione dei dati
Amministratore delegato	Contatta l'amministratore dell'account di gestione per richiedere l'accesso
Member Account	Contatta l'account di gestione o l'amministratore delegato per l'accesso
Account autonomo	Abilita Cost Explorer e attendi 24 ore per l'elaborazione dei dati

Soluzione alternativa

Inserisci valori personalizzati in modalità di modifica.

Cross-account accesso non funzionante

Problema

L'account amministratore o membro delegato visualizza l'avviso «I dati di utilizzo dell'organizzazione non sono disponibili per questo account».

Esamina le seguenti cause comuni e le relative soluzioni:

Cross-account il ruolo non esiste nell'account di gestione

Contatta l'amministratore dell'account di gestione per creare il ruolo. Lo strumento di stima dei costi fornisce istruzioni di configurazione guidate per gli utenti dell'account di gestione.

Il nome del ruolo non corrisponde esattamente

Nome del ruolo richiesto:`AwsSecurityHubCostEstimatorCrossAccountRole`. Verifica che il nome del ruolo nella console IAM corrisponda esattamente (con distinzione tra maiuscole e minuscole).

La politica di fiducia non consente il tuo account

Verifica che il principio principale della politica di fiducia includa l'ID dell'account e il nome del ruolo. Formato:`arn:aws:iam::{YOUR_ACCOUNT_ID}:role/{YOUR_ROLE_NAME}`.

AssumeRole Autorizzazione mancante

Verifica che il tuo responsabile IAM `sts:AssumeRole` disponga dell'autorizzazione. Contatta il tuo AWS amministratore per aggiungere questa autorizzazione.

Soluzione alternativa:

Inserisci valori personalizzati in modalità di modifica per stimare manualmente i costi senza i dati di Cost Explorer.

Ottenere istruzioni dettagliate

- Scegli Visualizza istruzioni nell'avviso per aprire un modale con:
  - Step-by-step guida alla configurazione
  - Pre-populated modelli di policy
  - Suggerimenti per la risoluzione dei problemi specifici relativi all'errore

Errori di autorizzazione

Problema

Errore «Accesso negato» per operazioni API specifiche.

Per risolvere gli errori di autorizzazione

1. Annota l'operazione negata contenuta nel messaggio di errore (ad esempio,`ce:GetCostAndUsage`).
2. Scegliete Copia per copiare i dettagli dell'errore.
3. Invia i dettagli dell'errore all' AWS amministratore.

4. Richiedi le autorizzazioni IAM richieste elencate in Autorizzazioni IAM richieste.

> **Note**
>
> Puoi comunque utilizzare la modalità di modifica per inserire valori manuali quando mancano le autorizzazioni, tranne quando l'accesso all'API Pricing è negato (impedisce tutte le stime dei costi).

La funzionalità indica «Non abilitato»

Problema

La funzionalità visualizza lo stato «Non abilitato».

Spiegazione

Questo stato viene visualizzato quando si dispone dell'accesso a Cost Explorer ma la funzionalità non è attualmente attiva. Se invece visualizzi $-/mo, significa che i dati di Cost Explorer non sono disponibili per il tuo tipo di account.

Per visualizzare le stime dei costi

1. Scegli Modifica per accedere alla modalità di modifica.
2. Immettete i valori delle dimensioni per la capacità.
3. Visualizza le stime dei costi aggiornate.

La funzionalità indica «Non applicabile»

Problema

La funzionalità visualizza «Non applicabile» nella colonna Servizi individuali.

Spiegazione

Questa funzionalità è disponibile solo tramite la tariffazione semplificata di Security Hub, non come servizio autonomo.

I costi modificati non corrispondono a Cost Explorer

Problema

I costi modificati sono diversi dai valori originali di Cost Explorer.

Spiegazione

Le stime modificate utilizzano le tariffe us-east-1 (Virginia settentrionale) e non includono sconti aziendali. I dati di Cost Explorer riflettono i costi effettivi con gli sconti applicabili.

Note importanti

- Le stime si basano sull'utilizzo osservato e fornito dall'utente e sulle informazioni pubbliche sui prezzi. I costi effettivi possono variare in base ai modelli di utilizzo e agli accordi aziendali
- Analisi retrospettiva di 30 giorni: i dati di Cost Explorer riflettono gli ultimi 30 giorni di utilizzo
- Regione dei prezzi: tutte le stime utilizzano le tariffe us-east-1 (Virginia settentrionale)
- Nessun impatto sulle impostazioni: le modifiche allo stimatore non influiscono sulle attuali configurazioni del Security Hub o del servizio
- Sconti aziendali: le stime modificate non includono gli sconti aziendali; solo i dati di Cost Explorer riflettono i costi effettivamente scontati
- Aggiornamento dei dati: i dati di Cost Explorer vengono aggiornati quotidianamente; aggiorna la pagina per visualizzare i dati più recenti

Informazioni correlate

- AWS Prezzi di Security Hub
- AWS Guida utente di Cost Explorer
- AWS Riferimento all'API dei prezzi
- Abilitazione di Security Hub

Abilitazione del Security Hub

Puoi abilitare Security Hub per qualsiasi Account AWS. Questa sezione della documentazione descrive tutti i passaggi necessari per abilitare Security Hub per un' AWS organizzazione o un account autonomo.

> **Important**
>
> Quando abiliti AWS Security Hub, Security Hub utilizza i dati a sua disposizione (inclusi i risultati, i dati di configurazione, l'inventario del software e altri dati AWS dell'ambiente) per potenziare le funzionalità che attivi. Man mano che miglioriamo le funzionalità esistenti o ne aggiungiamo di nuove, Security Hub può attingere a dati aggiuntivi già a sua disposizione per offrire un'esperienza migliore, come una valutazione più accurata dell'impatto reale delle esposizioni nell'ambiente, senza costi aggiuntivi. Puoi gestire le integrazioni e le funzionalità abilitate in qualsiasi momento. Consulta la documentazione del Security Hub per i dettagli o contatta il team AWS del tuo account o l' AWS assistenza per qualsiasi domanda.

Per una breve dimostrazione di come abilitare Security Hub, guarda il seguente video: Security Hub Onboarding Walkthrough and Demo.

Abilita Security Hub per un AWS Organizzazione

Questa sezione include tre passaggi:

- Nella Fase 1, l'account di gestione AWS dell'organizzazione designa un amministratore delegato per la propria AWS organizzazione, crea la politica dell'amministratore delegato e, facoltativamente, abilita Security Hub per il proprio account.
- Nella Fase 2, l'amministratore delegato dell'organizzazione abilita Security Hub per il proprio account.
- Nella Fase 3, l'amministratore delegato dell'organizzazione configura tutti gli account dei membri dell'organizzazione, per Security Hub e altri servizi di sicurezza supportati.

Passaggio 1. Delegare un account amministratore e, facoltativamente, abilitare Security Hub nel AWS account di gestione dell'organizzazione

> **Note**
>
> Completa questo passaggio in una regione dell'account di gestione dell'organizzazione.

Quando si assegna l'account amministratore delegato per Security Hub, l'account che è possibile scegliere per l'amministratore delegato dipende da come è stato configurato un amministratore delegato per Security Hub CSPM. Se è stato configurato un amministratore delegato per Security Hub CSPM e tale account non è l'account di gestione dell'organizzazione, tale account viene impostato automaticamente come amministratore delegato di Security Hub e non è possibile scegliere un account diverso. Se l'account amministratore delegato per Security Hub CSPM è impostato come account di gestione dell'organizzazione o non lo è affatto, è possibile scegliere quale account assegnare come account amministratore delegato di Security Hub, ad eccezione dell'account di gestione dell'organizzazione.

Per informazioni sulla designazione di un amministratore delegato in Security Hub, vedere Designazione di un account amministratore delegato in Security Hub. Per informazioni sulla creazione della politica di amministratore delegato in Security Hub, vedere Creazione della politica di amministratore delegato in Security Hub.

Per designare un amministratore per Security Hub

1. Accedi al tuo AWS account con le credenziali dell'account di gestione AWS dell'organizzazione. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dalla home page di Security Hub, scegli Security Hub, quindi scegli Inizia.

3. Nella sezione Amministratore delegato, scegli un account amministratore in base alle opzioni fornite. Come procedura ottimale, utilizza lo stesso amministratore delegato per tutti i servizi di sicurezza per una governance coerente.
4. Scegli la casella di controllo Accesso affidabile. La scelta di questa opzione concede all'account amministratore delegato la possibilità di configurare determinate funzionalità, come la protezione GuardDuty da malware, sugli account dei membri. Se deselezioni questa opzione, Security Hub non può abilitare queste funzionalità per tuo conto e devi abilitarle direttamente tramite il servizio a cui è associata la funzionalità.
5. (Facoltativo) Per abilitare l'account, seleziona la casella per abilitare Security Hub per il tuo AWS account.
6. Per la politica dell'amministratore delegato, scegli una delle seguenti opzioni per aggiungere la dichiarazione sulla politica.

    a. (Opzione 1) Scegli Aggiorna questo per me. Seleziona la casella sotto l'informativa sulla politica per confermare che Security Hub crei automaticamente una politica di delega che concede tutte le autorizzazioni richieste all'amministratore delegato.

    b. (Opzione 2) Scegli Voglio allegarlo manualmente. Scegli Copia e allega. Nella AWS Organizations console, in Amministratore delegato per AWS Organizations, scegli Delegato e incolla la politica delle risorse nell'editor dei criteri di delega. Scegli Crea policy. Apri la scheda in cui ti trovi nella console Security Hub.
7. Scegli Configura.

Passaggio 2. Abilita Security Hub nell'account amministratore delegato

L'account amministratore delegato completa questo passaggio. Dopo che l'account di gestione AWS dell'organizzazione ha designato un amministratore delegato per la propria organizzazione, l'amministratore delegato deve abilitare Security Hub per il proprio account prima di abilitarlo per l'intera organizzazione. AWS

Per abilitare Security Hub nell'account amministratore delegato

1. Accedi al tuo AWS account con le tue credenziali di amministratore delegato. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dalla home page di Security Hub, scegli Inizia.
3. La sezione sulle funzionalità di sicurezza descrive le funzionalità che vengono automaticamente abilitate e incluse nel prezzo base per risorsa di Security Hub.

4. (Facoltativo) Per i tag, stabilite se aggiungere una coppia chiave-valore alla configurazione dell'account.
5. Scegli Enable Security Hub per completare l'abilitazione di Security Hub.
6. (Consigliato) dal popup scegli Configura la mia organizzazione e procedi al passaggio 3.

Fase 3. Crea una politica che abiliti Security Hub in tutti gli account dei membri

Dopo aver abilitato Security Hub nell'account amministratore delegato di un'organizzazione, è necessario creare una politica che definisca quali servizi e funzionalità sono abilitati negli account dei membri dell'organizzazione. Per ulteriori informazioni, vedere Abilitazione di una configurazione con un tipo di politica.

Dopo aver abilitato Security Hub, nel tuo account vengono create le seguenti risorse:

- Un ruolo collegato al servizio chiamato. AWSServiceRoleForSecurityHubV2
- Service-linked registratori di configurazione. Per maggiori dettagli, consulta il Service-linked registratore nella documentazione sui concetti del Security Hub.
- Un analizzatore collegato ai servizi. Per maggiori dettagli, consulta Service-linked Analyzer nella documentazione sui concetti di Security Hub.

Abilitare Security Hub in un account autonomo

Questa procedura descrive come abilitare Security Hub in un account autonomo. Un account autonomo è un account Account AWS che non ha abilitato AWS le organizzazioni.

Per abilitare Security Hub in un account autonomo

1. Accedi al tuo AWS account con le credenziali del tuo account. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dalla home page di Security Hub, scegli Inizia.
3. Nella sezione Funzionalità di sicurezza, esegui una delle seguenti operazioni:

    a. (Opzione 1) Scegli Abilita tutte le funzionalità. Ciò attiva tutte le funzionalità essenziali del Security Hub, l'analisi delle minacce e le funzionalità aggiuntive.

    b. (Opzione 2) Scegli le funzionalità di personalizzazione. Seleziona le funzionalità da attivare nelle sezioni Gestione della sicurezza, Analisi delle minacce e Gestione delle vulnerabilità.

Non è possibile deselezionare alcuna funzionalità che fa parte delle funzionalità del piano essenziale di Security Hub.

4. Nella sezione Regioni, scegli Abilita tutte le regioni o Abilita regioni specifiche. Se scegli Abilita tutte le regioni, puoi determinare se abilitare automaticamente le nuove regioni. Se scegli Abilita regioni specifiche, devi scegliere quali regioni vuoi abilitare.
5. (Facoltativo) Per i tag Resource, aggiungete i tag come coppie chiave-valore per identificare facilmente la configurazione.
6. Scegliere Enable Security Hub (Abilita Security Hub).

Dopo aver abilitato Security Hub, le seguenti risorse vengono create in ogni account in cui è stato abilitato il servizio:

- Un ruolo collegato al servizio chiamato. AWSServiceRoleForSecurityHubV2
- Service-linked registratori di configurazione. Per maggiori dettagli, consulta il Service-linked registratore nella documentazione sui concetti del Security Hub.
- Un analizzatore collegato ai servizi. Per maggiori dettagli, consulta Service-linked Analyzer nella documentazione sui concetti di Security Hub.

Designazione di un amministratore delegato in Security Hub

Nell'account di gestione AWS dell'organizzazione, puoi designare un amministratore delegato per la tua organizzazione. Come best practice, utilizza lo stesso amministratore delegato per tutti i servizi di sicurezza per una governance coerente.

La procedura in questo argomento descrive come designare un amministratore delegato in Security Hub. Presuppone che tu abbia precedentemente abilitato Security Hub ma non abbia designato un amministratore delegato durante il flusso di lavoro di abilitazione.

Considerazioni

Quando si designa un amministratore delegato in Security Hub, si consideri quanto segue:

- L'account di gestione AWS dell'organizzazione può designarsi come amministratore delegato in Security Hub CSPM, ma non può designarsi come amministratore delegato in Security Hub. In questo scenario, l'account di gestione deve designarne un altro Account AWS come amministratore delegato in Security Hub.

- Se l'account di gestione AWS dell'organizzazione designa un amministratore delegato in Security Hub CSPM, tale amministratore delegato diventa automaticamente l'amministratore delegato in Security Hub. In questo scenario, Security Hub consente solo a questo particolare di fungere Account AWS da amministratore delegato.

> **Note**
>
> La rimozione dell'amministratore delegato tramite la console Security Hub CSPM, la console Security Hub o l' AWS Organizations API lo rimuove da entrambi i servizi. Quando l'amministratore delegato viene rimosso da Security Hub CSPM, Central Configuration viene automaticamente disattivato.

Designazione di un amministratore delegato dopo l'attivazione di Security Hub

Questa procedura deve essere completata dall'account di gestione AWS dell'organizzazione. Presuppone che l'account di gestione AWS dell'organizzazione abbia precedentemente abilitato Security Hub ma non abbia designato un amministratore delegato durante il flusso di lavoro di abilitazione.

> **Note**
>
> Dopo aver completato questa procedura, è necessario creare una policy che consenta all'amministratore delegato dell'organizzazione di configurare Security Hub ed eseguire azioni specifiche in. AWS Organizations Per ulteriori informazioni, vedere Creazione della politica dell'amministratore delegato in Security Hub.

Per designare un amministratore delegato in Security Hub

1. Accedi al tuo AWS account con le credenziali dell'account di gestione dell'organizzazione e apri la console Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
2. Dal pannello di navigazione, scegli Generale.
3. In Amministratore delegato, scegli Configura. Seleziona uno dei dati forniti Account AWS o inserisci il Account AWS numero di 12 cifre Account AWS che desideri designare come amministratore delegato per la tua organizzazione. Scegli Save (Salva).

Creazione della politica dell'amministratore delegato in Security Hub

L'account di gestione AWS dell'organizzazione può creare una policy che consenta all'amministratore delegato di configurare Security Hub ed eseguire azioni specifiche in AWS Organizations. La procedura in questo argomento descrive come creare la policy. Al termine della procedura, puoi consentire a Security Hub di creare la policy per te o di crearla manualmente. Consenti a Security Hub di creare la policy a meno che tu non voglia personalizzarla per un caso d'uso particolare.

Completa questa procedura solo se l'account di gestione dell'organizzazione ha abilitato Security Hub e designato un amministratore delegato, ma ha saltato la creazione della policy durante il flusso di lavoro di abilitazione. Per informazioni su come aggiornare questa politica, consulta Aggiornare una politica di delega basata sulle risorse nella Guida per l'utente. AWS Organizations AWS Organizations

> **Note**
>
> Dopo aver completato questa procedura, l'amministratore delegato può creare una policy per gestire gli account dei membri nell'organizzazione. Per ulteriori informazioni, vedere Creazione di una policy come amministratore delegato per la gestione degli account dei membri.

Per creare la politica dell'amministratore delegato

1. Accedi al tuo AWS account con le credenziali dell'account di gestione dell'organizzazione. Apri la console Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
2. Dal pannello di navigazione, scegli Generale.
3. Per la politica degli amministratori delegati, esegui una delle seguenti operazioni:
   - Scegli Crea policy. Seleziona la casella sotto la dichiarazione della politica per confermare che Security Hub crea automaticamente una politica di delega che concede tutte le autorizzazioni richieste all'amministratore delegato.
   - Apri la policy. Scegli Copia e allega. Nella AWS Organizations console, in Amministratore delegato per AWS Organizations, scegli Delegato e incolla la politica delle risorse nell'editor dei criteri di delega. Scegli Crea policy. Apri la scheda in cui ti trovi nella console di Security Hub e scegli Configura.

Gestione della configurazione degli account dei membri in un AWS Organizzazione

L'amministratore delegato di un' AWS organizzazione può configurare le funzionalità di sicurezza tra gli account dei membri e le regioni. Sono disponibili due tipi di configurazioni: politiche e implementazioni. Le policy generano le policy AWS delle organizzazioni per gli account e le regioni per AWS Security Hub e Amazon Inspector. Le implementazioni sono un'azione una tantum per abilitare una funzionalità di sicurezza tra account e regioni selezionati per Amazon GuardDuty e AWS Security Hub CSPM. A differenza delle policy, non è possibile visualizzare o modificare le distribuzioni e le distribuzioni non si applicano ai nuovi account abilitati. In alternativa, le funzionalità di attivazione automatica per i nuovi account membri sono disponibili in Amazon GuardDuty e AWS Security Hub CSPM.

Catalogo di configurazione di Security Hub

Il catalogo di configurazione di Security Hub offre diverse opzioni per aiutare a configurare gli account AWS dell'organizzazione per le funzionalità di sicurezza fornite da Security Hub.

Le seguenti sono le opzioni disponibili nel catalogo di configurazione di Security Hub.

Security Hub (funzionalità essenziali e aggiuntive)

Questa è la configurazione consigliata da implementare per Security Hub.

Tipo: Policy e implementazioni

Descrizione: questa configurazione attiva le funzionalità essenziali di gestione della sicurezza, gestione della postura, analisi delle minacce e gestione delle vulnerabilità di Security Hub. Facoltativamente, abilita funzionalità aggiuntive.

Analisi delle minacce da GuardDuty

Tipo: Implementazione

Descrizione: attiva GuardDuty le funzionalità Amazon selezionate per monitorare, analizzare ed elaborare continuamente le fonti di AWS dati e i log nel tuo AWS ambiente.

Gestione della postura da AWS Security Hub CSPM

Tipo: distribuzione

Descrizione: questa configurazione attiva gli standard e i controlli di Security Hub CSPM, che rilevano quando gli AWS account e le risorse si discostano dalle best practice di sicurezza.

Gestione delle vulnerabilità da Amazon Inspector

Tipo: Policy

Descrizione: questa configurazione attiva funzionalità selezionate di Amazon Inspector che rilevano automaticamente carichi di lavoro, istanze, immagini di container e altre risorse e li analizza per individuare vulnerabilità ed esposizione alla rete.

Abilitazione di una configurazione con un tipo di policy

La procedura seguente descrive come creare una configurazione con un tipo di policy per gli account AWS dell'organizzazione. Per creare una politica di configurazione, è necessario innanzitutto creare la politica dell'amministratore delegato nell'account di gestione dell' AWS organizzazione. Per informazioni sulla creazione della politica dell'amministratore delegato in Security Hub, vedere Creazione della politica dell'amministratore delegato in Security Hub.

Per creare una policy che abiliti e disabiliti gli account dei membri

1. Accedi utilizzando il tuo AWS account con le tue credenziali di amministratore delegato. Apri la console Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
2. Dal pannello di navigazione, scegli Gestione, quindi scegli Configurazioni.
3. Scegli un elemento con un tipo di policy o policy e distribuzione dal catalogo di configurazione. Per configurare completamente Security Hub, scegli Security Hub (funzionalità essenziali e aggiuntive).
4. Nella pagina Configura Security Hub, nella sezione Dettagli, inserisci un nome e una descrizione per la policy.
5. Nella sezione Funzionalità di sicurezza, scegli una delle seguenti opzioni:
   - Abilita tutte le funzionalità: attiva tutte le funzionalità essenziali di Security Hub, l'analisi delle minacce e le funzionalità aggiuntive.
   - Personalizza le funzionalità: seleziona le funzionalità dalle sezioni Gestione della sicurezza, Analisi delle minacce e Gestione delle vulnerabilità. Non è possibile deselezionare le funzionalità che fanno parte del piano Security Hub essential.
6. Nella sezione Selezione dell'account, scegli una delle seguenti opzioni:
   - Tutte le unità organizzative e gli account: applica la configurazione all'intera organizzazione.

- Unità organizzative e account specifici: utilizza la barra di ricerca o l'albero della struttura organizzativa per selezionare le unità organizzative e gli account a cui si applica la politica.
- Nessuna unità organizzativa o account: non applica la configurazione a nessuna unità organizzativa o account.

7. Nella sezione Regioni, scegli una delle seguenti opzioni:
   - Abilita tutte le regioni: opzionalmente, scegli se abilitare automaticamente le nuove regioni.
   - Disabilita tutte le regioni: opzionalmente, scegli se disabilitare automaticamente le nuove regioni.
   - Specifica le regioni: scegli quali regioni abilitare e disabilitare.
8. (Facoltativo) Per le impostazioni avanzate, vedere Operatori di ereditarietà nella Guida per l'AWS Organizations utente.
9. (Facoltativo) Per i tag Resource, aggiungete i tag come coppie chiave-valore per aiutarvi a identificare la configurazione.
10. Scegli Next (Successivo).
11. Rivedi le modifiche, quindi scegli Applica.

    Lo stato di configurazione della politica viene visualizzato nella parte superiore della pagina Politiche. Ogni funzionalità fornisce uno stato che indica se è stata configurata correttamente o presenta errori di distribuzione. Per eventuali errori, scegli il link relativo all'errore per visualizzare maggiori dettagli. Per visualizzare la politica efficace a livello di account, consulta la scheda Organizzazione nella pagina Configurazioni.

Abilitazione di una configurazione con un tipo di distribuzione

La procedura seguente descrive come creare una configurazione con un tipo di distribuzione per gli account AWS dell'organizzazione.

Per creare una distribuzione che abiliti gli account dei membri

1. Accedi utilizzando il tuo AWS account con le tue credenziali di amministratore delegato. Apri la console Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
2. Dal pannello di navigazione, scegli Gestione, quindi scegli Configurazioni.
3. Scegli un elemento con un tipo di distribuzione dal catalogo di configurazione.
4. Nella sezione Funzionalità di sicurezza, seleziona le funzionalità di sicurezza da attivare.

5. Nella sezione Selezione dell'account, scegli una delle seguenti opzioni:
   - Tutte le unità organizzative e gli account: applica la distribuzione all'intera organizzazione.
   - Unità organizzative e account specifici: utilizza la barra di ricerca o l'albero della struttura organizzativa per selezionare le unità organizzative e gli account a cui si applica la distribuzione.
   - Nessuna unità organizzativa o account: non applica la distribuzione a nessuna unità organizzativa o account.
6. Nella sezione Regioni, scegli una delle seguenti opzioni:
   - Abilita tutte le regioni: opzionalmente, scegli se abilitare automaticamente le nuove regioni.
   - Disabilita tutte le regioni: opzionalmente, scegli se disabilitare automaticamente le nuove regioni.
   - Specifica le regioni: scegli quali regioni abilitare e disabilitare.
7. Scegli Configura.

Modifica di una politica di configurazione

È possibile modificare le funzionalità, le regioni e gli account associati a una politica di configurazione. Quando si apre una policy per la modifica, la console mostra la configurazione corrente.

> **Note**
>
> Le modifiche si applicano solo alle funzionalità selezionate nella policy aggiornata. Le funzionalità non selezionate mantengono la configurazione esistente per tutti gli account e le aree geografiche inclusi nella policy.

Per modificare una politica di configurazione

1. Accedi utilizzando il tuo AWS account con le credenziali di amministratore delegato. Apri la console Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
2. Dal pannello di navigazione, scegli Gestione, quindi scegli Configurazioni.
3. Nella scheda Criteri configurati, scegli il pulsante di opzione relativo al criterio che desideri modificare, quindi scegli Modifica.

4. Nella sezione Capacità, scegli una delle seguenti opzioni:
   - Configura e abilita tutte le funzionalità: abilita tutte le funzionalità della policy.
   - Seleziona le singole funzionalità e scegli Abilita , Disabilita o Personalizzata per ognuna.
5. Nella sezione Selezione dell'account, scegli una delle seguenti opzioni:
   - Tutte le unità organizzative e gli account: applica la politica all'intera organizzazione.
   - Unità organizzative e account specifici: utilizza la barra di ricerca o l'albero della struttura organizzativa per selezionare le unità organizzative e gli account a cui si applica la politica.
   - Nessuna unità organizzativa o account: rimuove la politica da tutti gli obiettivi.
6. Nella sezione Regioni, configura a quali regioni si applica la policy. Le opzioni dipendono dalle capacità selezionate.

   Se hai scelto di abilitare tutte le funzionalità:
   - Per tutte le funzionalità selezionate: imposta la stessa configurazione regionale per tutte le funzionalità.
   - Per funzionalità: consente di scegliere le regioni individualmente per ciascuna funzionalità.

   Quindi scegli Abilita tutte le regioni (con l'opzione per abilitare automaticamente le nuove regioni) o Abilita in alcune regioni per selezionare regioni specifiche.

   Se hai scelto azioni miste (abilita, disabilita o personalizzata) per le singole funzionalità:
   - Se tutte le funzionalità selezionate condividono la stessa azione, scegli Tra tutte le funzionalità selezionate per impostare le regioni in modo uniforme. Per impostare le regioni per ciascuna capacità singolarmente, scegli Per capacità.
   - Se le funzionalità hanno azioni diverse, è necessario assegnare le regioni a ciascuna capacità singolarmente.
   - Per le funzionalità con l'azione Personalizzata, scegli Tra tutte le funzionalità selezionate per impostare le regioni in modo uniforme per tutte le funzionalità. Per configurare le regioni per ciascuna funzionalità separatamente, scegli Per funzionalità.
7. Scegli Next (Successivo).
8. Rivedere le modifiche, quindi scegliere Update (Aggiorna). La policy aggiornata configura gli account di destinazione.

Eliminazione di una politica di configurazione

È possibile eliminare una politica di configurazione. Quando si elimina una policy, il servizio rimuove tutti gli account e le unità organizzative collegati dalla policy.

Come eliminare una policy di configurazione

1. Accedi utilizzando il tuo AWS account con le credenziali di amministratore delegato. Apri la console Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
2. Dal pannello di navigazione, scegli Gestione, quindi scegli Configurazioni.
3. Nella scheda Criteri configurati, seleziona il criterio che desideri eliminare, quindi scegli Elimina.
4. Inserisci `delete` nella casella di conferma, quindi scegli Elimina.

Rimozione dell'account amministratore delegato in Security Hub

È possibile rimuovere l'account amministratore delegato nella console Security Hub in qualsiasi momento. Tuttavia, questa azione rimuove l'amministratore delegato sia da Security Hub che da Security Hub CSPM. Ti consigliamo di eseguire questa azione solo dopo aver confermato l'operazione con il tuo account di sicurezza.

> **Note**
>
> Se si utilizza un account diverso dall'account di gestione dell'organizzazione come amministratore delegato CSPM di Security Hub, rimuoverlo tramite la console Security Hub CSPM o l' AWS Organizations API lo rimuove anche da Security Hub.
> Analogamente, se si rimuove l'amministratore delegato di Security Hub tramite la console di Security Hub o l' AWS Organizations API, questo viene rimosso anche da Security Hub CSPM. Quando l'amministratore delegato viene rimosso da Security Hub CSPM, Central Configuration viene automaticamente disattivato.

Per rimuovere l'account amministratore delegato

1. Accedi al tuo AWS account con le credenziali dell'account di gestione dell'organizzazione. Apri la console Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
2. Dal pannello di navigazione, scegli Generale.

3. In Amministratore delegato, scegli Rimuovi amministratore delegato. Nella finestra di dialogo di conferma, inserisci remove e scegli Rimuovi.

Re-enabling Hub di sicurezza

Prima di riattivare Security Hub sugli account precedentemente disattivati utilizzando una policy di Security Hub, devi prima scollegare la policy di disabilitazione. Se si tenta di riattivare Security Hub mentre un criterio di disattivazione è ancora associato all'account o all'unità organizzativa, il criterio di disabilitazione prevale sull'abilitazione e Security Hub rimane disabilitato.

Per rimuovere il criterio di disattivazione di Security Hub per un'organizzazione o un account

1. Accedi utilizzando il tuo AWS account con le credenziali dell'account di gestione dell'organizzazione. Apri la AWS Organizations console all'indirizzo. https://console.aws.amazon.com/organizations/v2/home
2. Dal pannello di navigazione scegli AWS account.
3. Se l'attuale politica di disabilitazione di Security Hub riguardava l'intera organizzazione, scegli Root nella struttura organizzativa. Se l'attuale politica di disabilitazione di Security Hub riguarda account specifici, scegli l'account specifico nella Struttura organizzativa e segui i passaggi rimanenti per ciascun account.
4. Nella scheda Politiche, trova la sezione intitolata Politiche di Security Hub.
5. Scegli il pulsante di opzione accanto alla policy che disabilita Security Hub. Seleziona Scollega.

Dopo aver rimosso la policy dalla tua organizzazione o dai tuoi account, puoi riattivare Security Hub. Vedi Gestione della configurazione degli account dei membri in un' AWS organizzazione per i dettagli sulla riattivazione di Security Hub.

Raccomandazioni sul Security Hub

I seguenti servizi di sicurezza AWS inviano i risultati a Security Hub nel formato OCSF. Dopo aver abilitato Security Hub, abilitalo Servizi AWS per una maggiore sicurezza.

Security Hub CSPM

Quando abiliti Security Hub CSPM, ottieni una visione completa del tuo stato di sicurezza in. AWS Questo ti aiuta a valutare il tuo ambiente rispetto agli standard e alle best practice del settore della sicurezza. Sebbene sia possibile iniziare a utilizzare Security Hub senza abilitare Security Hub

CSPM, l'attivazione di Security Hub CSPM consente a Security Hub di correlare i segnali di sicurezza di Security Hub CSPM per migliorare la gestione della postura.

Se abiliti Security Hub CSPM, ti consigliamo anche di abilitare lo standard AWS Foundational Security Best Practices per il tuo account. Questo standard consiste in una serie di controlli che rilevano quando le tue risorse Account AWS e le tue risorse si discostano dalle migliori pratiche di sicurezza. Quando abiliti lo standard AWS Foundational Security Best Practices per il tuo account, AWS Security Hub CSPM abilita automaticamente tutti i suoi controlli, inclusi i controlli per i seguenti tipi di risorse:

- Controlli dell'account
- Controlli Amazon DynamoDB
- Controlli Amazon Elastic Compute Cloud
- AWS Identity and Access Management controlli (IAM)
- AWS Lambda controlli
- Controlli di Amazon Relational Database Service (Amazon RDS)
- Controlli di Amazon Simple Storage Service

Puoi disabilitare qualsiasi controllo in questo elenco. Tuttavia, se si disabilita uno di questi controlli, non è possibile ricevere i risultati sull'esposizione per le risorse supportate. Per informazioni sui controlli che si applicano allo standard AWS Foundational Security Best Practices, consulta lo standard AWS Foundational Security Best Practices v1.0.0 (FSBP).

GuardDuty

Quando abiliti GuardDuty, puoi visualizzare tutte le minacce e i risultati della copertura di sicurezza nella dashboard della console Security Hub. Se abiliti GuardDuty, inizia GuardDuty automaticamente a inviare dati a Security Hub nel formato OCSF.

Amazon Inspector

Quando attivi Amazon Inspector, puoi visualizzare tutte le esposizioni e i risultati della copertura di sicurezza nella dashboard della console Security Hub. Se abiliti Amazon Inspector, Amazon Inspector inizia automaticamente a inviare dati a Security Hub nel formato OCSF.

Consigliamo di attivare la scansione Amazon EC2 e la scansione standard Lambda. Quando attivi la scansione di Amazon EC2, Amazon Inspector analizza le istanze Amazon EC2 nel tuo account alla

ricerca di vulnerabilità dei pacchetti e problemi di raggiungibilità della rete. Quando attivi la scansione standard Lambda, Amazon Inspector analizza le funzioni Lambda alla ricerca di vulnerabilità software nelle dipendenze dei pacchetti. Per ulteriori informazioni, consulta Attivazione di un tipo di scansione nella Guida per l'utente di Amazon Inspector.

Macie

Quando abiliti Macie, puoi rilevare esposizioni aggiuntive per i tuoi bucket Amazon S3. Ti consigliamo di configurare il rilevamento automatico dei dati sensibili, in modo che Macie possa valutare il tuo inventario di bucket Amazon S3 su base giornaliera.

Copertura dell'account in Security Hub

La pagina di copertura dell'account mostra per quali account e regioni dell'organizzazione sono abilitati Security Hub e le sue funzionalità di sicurezza integrate. Queste funzionalità includono servizi come Amazon Inspector GuardDuty, Amazon, AWS Security Hub CSPM e Amazon Macie. Utilizza questa pagina per identificare le lacune di copertura e monitorare l'adozione delle funzionalità in tutta l'organizzazione.

Pagina di copertura dell'account

Con la pagina di copertura dell'account, puoi visualizzare le metriche di copertura aggregate. Utilizza la scheda Account per i dettagli a livello di account e la scheda Risultati della copertura per esaminare le lacune di copertura specifiche.

Per accedere al Security Hub Copertura dell'account page

1. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal pannello di navigazione, in Impostazioni scegli Copertura dell'account.

Sezione panoramica

La sezione Panoramica mostra le metriche di copertura di sicurezza aggregate per tutti gli account monitorati. Per gli account amministratore delegato, questa sezione mostra i dettagli di attivazione del Security Hub in tutta l'organizzazione, fornendo visibilità sulla copertura per tutti gli account dei membri. Questa visualizzazione di alto livello mostra la percentuale di account con Security Hub e ogni funzionalità di sicurezza abilitata, offrendo una visione completa del tuo livello di sicurezza. È

possibile selezionare la percentuale di copertura del Security Hub per visualizzare una ripartizione degli account abilitati per regione. È possibile selezionare ogni percentuale di capacità per filtrare i risultati della copertura in base a tale capacità.

Le percentuali nella sezione Panoramica sono determinate utilizzando i seguenti calcoli:

- Attivazione Security Hub = (Numero di coppie di account e regioni in cui Security Hub è abilitato) ÷ (Account totali nell'organizzazione × Regioni in cui è disponibile Security Hub)
- Copertura dei servizi = (Numero di account abilitati e coppie di regioni configurate in cui la funzionalità è abilitata) ÷ (Numero totale di account abilitati e coppie di regioni configurate, nelle regioni configurate in cui l'account è abilitato e la funzionalità è disponibile)

> **Regioni configurate**
>
> Per la configurazione della regione principale, le regioni configurate includono la regione d'origine e le regioni collegate. Per tutte le altre configurazioni, le regioni configurate si riferiscono solo alla regione corrente.

Scheda Account

Questa scheda è disponibile solo nell'account amministratore delegato di Security Hub. Utilizza la scheda Account per analizzare la copertura specifica dell'account. La colonna Security Hub mostra il numero di regioni in cui Security Hub è abilitato per ogni account. Questa colonna non viene visualizzata quando si visualizza la scheda nelle regioni opzionali (regioni disabilitate per impostazione predefinita). Ogni funzionalità di sicurezza mostra una percentuale di copertura che, se selezionata, rivela un'analisi dettagliata delle singole funzionalità e della relativa percentuale di copertura all'interno di tale funzionalità. Quando selezioni queste percentuali, Security Hub filtra i risultati per visualizzare la copertura per quella funzionalità e l'account.

Le percentuali nella scheda Account vengono determinate utilizzando il seguente calcolo:

Copertura della scheda Account = (Numero di regioni in cui la funzionalità è abilitata) ÷ (Regioni in cui la funzionalità è disponibile)

Esistono diversi casi in cui la percentuale di copertura potrebbe essere dello 0%:

- Security Hub non è abilitato nell'account e quindi non vengono acquisiti i risultati della copertura.

- Security Hub è in attesa che vengano generati i risultati della copertura.

Scheda dei risultati della copertura

La scheda Risultati della copertura elenca i risultati informativi relativi alle funzionalità di sicurezza abilitate o disabilitate in tutti gli account e le aree geografiche. Questi risultati aiutano a identificare le aree in cui è possibile migliorare la copertura di sicurezza. Ogni risultato mostra il titolo del risultato, l'account e la regione interessati e lo stato attuale. Ogni risultato ha anche un collegamento di configurazione che porta al servizio individuale in cui è possibile gestire la configurazione per tale funzionalità o alla pagina delle configurazioni del Security Hub in cui è possibile aggiornare le configurazioni per i servizi di sicurezza.

Puoi eliminare i risultati della copertura con lo stato Non coperto se tale funzionalità di sicurezza non è applicabile alla combinazione Account/area geografica. Security Hub esclude i risultati soppressi dal calcolo della percentuale di copertura di sicurezza.

Per ulteriori informazioni sui risultati della copertura e su come eliminarli, consulta Risultati della copertura in Security Hub.

Widget di copertura di sicurezza

La copertura dell'account può essere visualizzata anche tramite il widget Copertura di sicurezza nella dashboard di riepilogo di Security Hub. Per ulteriori informazioni, consulta Widget di copertura di sicurezza.

Piano Security Hub Extended

Con il piano Security Hub Extended, puoi proteggere l'intero patrimonio aziendale su cloud, endpoint, rete, identità, dati, email e browser. Usa AWS Security Hub come centro di un'esperienza operativa di sicurezza integrata. Con il piano Security Hub Extended, puoi selezionare le soluzioni dei partner che rispondono alle tue esigenze di sicurezza e sottoscrivere prezzi flessibili con pagamento in base al consumo senza investimenti iniziali o impegni a lungo termine. Puoi aggiungere o rimuovere soluzioni partner man mano che le tue esigenze aziendali si evolvono.

Il piano Security Hub Extended è disponibile per tutti i clienti che hanno abilitato il piano Security Hub Essentials. Gli addebiti per il piano Security Hub Extended vengono visualizzati nella AWS fattura mensile con AWS la dicitura «venditore registrato».

I prezzi del piano Security Hub Extended per tutte le soluzioni sono disponibili nella scheda Piano esteso della pagina dei dettagli dei prezzi di Security Hub.

Autorizzazioni per il piano Security Hub Extended

Per abbonarti a un prodotto partner del piano Security Hub Extended, sono necessarie le seguenti autorizzazioni, oltre alle autorizzazioni Security Hub:

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

Per annullare l'iscrizione a un prodotto partner incluso nel piano Security Hub Extended, sono necessarie le seguenti autorizzazioni, oltre alle autorizzazioni Security Hub:

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

Per ulteriori informazioni sulle autorizzazioni di AWS Marketplace, consulta Controllare l'accesso agli abbonamenti di Marketplace nella AWS Marketplace Buyer Guide. AWS

Revisione e iscrizione ai partner del piano esteso

Il piano Security Hub Extended è accessibile tramite l'account amministratore delegato di Security Hub o account autonomi. Nella pagina del piano Security Hub Extended, puoi visualizzare i dettagli su ciascun partner, avviare un abbonamento a una soluzione partner e iniziare il processo di onboarding per la soluzione di ciascun partner tramite la pagina di onboarding del partner.

Per accedere al piano Security Hub Extended e iscriverti al prodotto di un partner

1. Accedi alla console di AWS gestione utilizzando le credenziali dell'amministratore delegato o dell'account autonomo.
2. Aprire la console Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
3. Nel pannello di navigazione, scegli Gestione, quindi scegli Piano esteso.
4. Per ogni soluzione partner a cui desideri iscriverti, scegli Visualizza prodotto.

5. Controlla i dettagli dei prezzi del prodotto, quindi scegli Abbonati quando sei pronto per iniziare il processo di onboarding del prodotto partner.
6. Una volta completato il processo di abbonamento, scegli Configura il tuo account per essere reindirizzato alla pagina di registrazione del partner.
7. Fornisci le informazioni necessarie per la pagina di iscrizione del partner e segui i passaggi successivi, forniti dal partner, per completare i passaggi di onboarding.

> **Important**
>
> La soluzione partner non ti verrà fatturata finché non avrai completato la procedura di onboarding per il prodotto partner.

Annullamento dell'iscrizione a un partner del piano esteso

Se non desideri più utilizzare una soluzione partner con piano esteso, puoi annullare l'iscrizione all'elenco dei partner.

Per annullare l'iscrizione a una soluzione partner, segui le indicazioni riportate nella sezione Annullamento dell'abbonamento SaaS nella Marketplace Buyer Guide. AWS

> **Important**
>
> Oltre all'annullamento dell'abbonamento, segui tutte le ulteriori fasi di offboarding necessarie per la soluzione partner, in base a come hai configurato la soluzione per la tua azienda.

Comprendere l'aggregazione interregionale in Security Hub

Quando abiliti l'aggregazione tra regioni in Security Hub, definisci una regione di origine. La regione d'origine raccoglie risultati, risorse e tendenze da una o più regioni collegate. È quindi possibile gestire tutti i dati di sicurezza da una singola regione.

Supponiamo di impostare Stati Uniti orientali (Virginia settentrionale) come regione di origine e Stati Uniti occidentali (Oregon) e Stati Uniti occidentali (California settentrionale) come regioni collegate. Quando si visualizza la pagina Risultati negli Stati Uniti orientali (Virginia settentrionale), vengono

visualizzati i risultati di tutte e tre le regioni. Gli aggiornamenti a tali risultati si riflettono anche in tutte e tre le regioni.

Tipi di dati aggregati

Quando l'aggregazione tra regioni è abilitata con una o più regioni collegate, Security Hub replica i seguenti dati dalle regioni collegate alla regione principale. Ciò si verifica in tutti gli account in cui è abilitata l'aggregazione tra regioni.

- Esiti
- Resources
- Tendenze
- Inventario di software e pacchetti (a partire da novembre 2026)

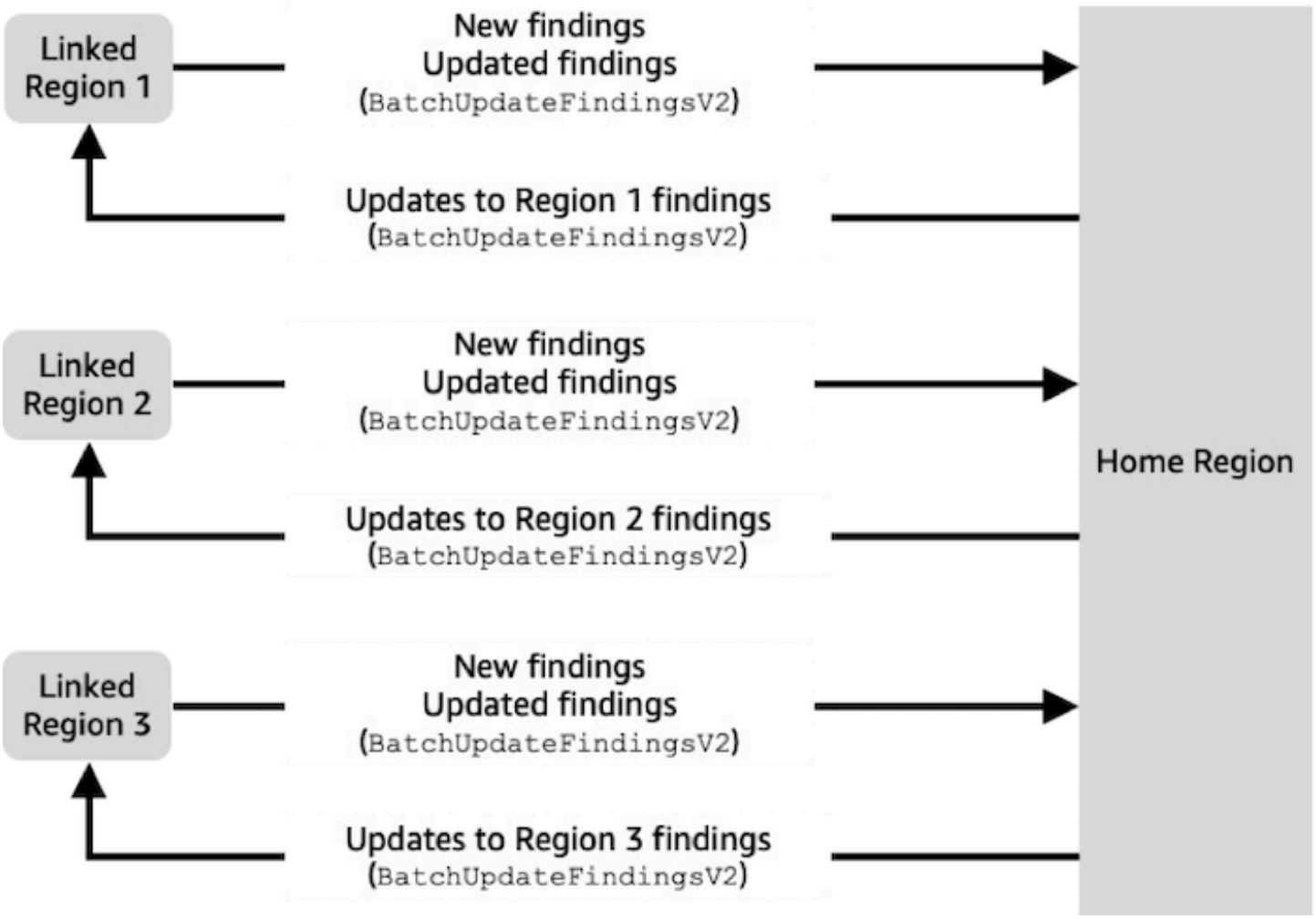
Oltre ai nuovi dati nell'elenco precedente, Security Hub replica anche gli aggiornamenti di questi dati tra le regioni collegate e la regione di origine. Gli aggiornamenti che si verificano in una regione collegata vengono replicati nella regione di origine. Gli aggiornamenti che si verificano nella regione di origine vengono replicati nella regione collegata. Se sono presenti aggiornamenti in conflitto nella regione di origine e nella regione collegata, viene utilizzato l'aggiornamento più recente.

Qualsiasi risultato esistente in una regione nel momento in cui diventa una regione collegata non viene replicato nella regione d'origine a meno che non vi sia un aggiornamento del risultato. Dopo che una regione è stata collegata a una regione d'origine, esiste una differenza nei risultati tra la regione d'origine e la regione collegata fino a quando i risultati nella regione collegata non vengono aggiornati o non scadono.

Tutte le risorse esistenti in una regione nel momento in cui diventa una regione collegata vengono replicate nella regione d'origine, in genere entro 24-48 ore dal collegamento della regione a una regione d'origine.

Quando si rimuove una regione collegata, tutte le scoperte o le risorse relative a quella regione rimangono nella regione d'origine fino all'esaurimento del reperto o della risorsa.

I dati sulle tendenze si basano su risultati e risorse presenti nella regione a cui si riferisce la tendenza. I dati sulle tendenze in una regione d'origine riflettono lo stato attuale dei risultati e delle risorse che sono stati sincronizzati con la regione d'origine.



Cross-Region l'aggregazione non aumenta il costo di Security Hub. Non ti viene addebitato alcun costo quando Security Hub replica nuovi dati o aggiornamenti.

Nella regione di origine, la pagina di riepilogo fornisce una visualizzazione dei risultati e delle risorse attivi nelle regioni collegate.

Security Hub aggrega solo i dati delle regioni in cui un account ha Security Hub abilitato. Security Hub non è abilitato automaticamente per un account in base alla configurazione di aggregazione tra regioni.

È possibile abilitare l'aggregazione tra regioni senza selezionare alcuna regione collegata. In questo caso, non si verifica alcuna replica dei dati.

Aggregazione per gli account degli amministratori e dei membri

Gli account autonomi e gli account amministratore possono configurare l'aggregazione tra regioni. Se configurata da un amministratore, la presenza dell'account amministratore è essenziale affinché l'aggregazione tra regioni funzioni negli account amministrati. Se l'account amministratore viene rimosso o dissociato da un account membro, l'aggregazione tra aree geografiche si interrompe per quell'account membro. Tuttavia, se l'account membro aveva una propria configurazione di aggregazione tra aree geografiche prima di essere associato a un amministratore, tale configurazione torna in vigore.

Quando un account amministratore abilita l'aggregazione tra regioni, Security Hub replica i dati generati dall'account amministratore in tutte le regioni collegate alla regione di origine. Inoltre, Security Hub identifica gli account membro associati a quell'amministratore e ogni account membro eredita le impostazioni di aggregazione interregionale dell'amministratore. Security Hub replica i dati generati da un account membro in tutte le regioni collegate alla regione di origine.

L'amministratore può accedere e gestire i risultati di sicurezza di tutti gli account dei membri all'interno delle Regioni amministrate. Inoltre, l'amministratore può visualizzare l'inventario delle risorse di tutti gli account membri all'interno delle Regioni amministrate.

In qualità di account membro di Security Hub, devi accedere alla regione di origine per visualizzare i dati aggregati del tuo account da tutte le regioni collegate. Gli account membro non dispongono delle autorizzazioni per visualizzare i dati degli altri account membri e non sono autorizzati a chiamare le API `CreateAggregatorV2DeleteAggregatorV2`, `eGetAggregatorV2`.

Regole di automazione e aggregazione tra regioni

Quando l'aggregazione tra regioni è abilitata, le regole di automazione possono essere create solo nella regione di origine definita. Qualsiasi regola definita si applica a tutte le regioni collegate, a meno che i criteri delle regole non si applichino a regioni specifiche. È necessario creare regole di automazione separate per qualsiasi regione che non sia una regione collegata.

Tutte le regole create nella regione di origine, prima di abilitare l'aggregazione tra regioni, diventano automaticamente applicabili nelle regioni collegate. Le regole create in precedenza nelle regioni collegate non verranno più applicate una volta creato un aggregatore. Le regole definite nelle regioni collegate riprenderanno ad applicarsi dopo l'eliminazione dell'aggregatore o dopo che la regione non è più collegata.

Abilitazione dell'aggregazione tra regioni

È necessario abilitare l'aggregazione tra regioni dalla AWS regione che si desidera designare come regione di origine.

Per abilitare l'aggregazione tra regioni, si crea una risorsa Security Hub denominata aggregatore di ricerca. La risorsa Finding Aggregator specifica la tua regione di origine e le regioni collegate (se presenti).

Non è possibile utilizzare come AWS regione di residenza una regione disattivata per impostazione predefinita. Per un elenco delle regioni che sono disabilitate per impostazione predefinita, vedi Abilitazione di una regione nella AWS Guida generale.

Quando abiliti l'aggregazione tra regioni, scegli di specificare una o più regioni collegate, se lo desideri. L'abilitazione dell'aggregazione tra regioni non abilita Security Hub in quella regione. Per abilitare Security Hub in una regione, consulta Creazione di una policy come amministratore delegato per la gestione degli account dei membri nella guida per l'utente di Security Hub.

Per abilitare l'aggregazione tra regioni (console)

1. Dall'account amministratore o in un account autonomo, apri la console AWS Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home
2. Utilizzando il selettore AWS della regione, accedi alla regione che desideri utilizzare come regione di aggregazione.
3. Nel menu di navigazione di Security Hub, scegli Impostazioni, quindi Generali.
4. Nella sezione di Cross-Region aggregazione, scegli Configura.
5. Per impostazione predefinita, la regione principale è impostata su Nessuna regione di aggregazione.
6. In Area geografica, seleziona l'opzione per designare la regione corrente come regione d'origine.
7. Facoltativamente, per le regioni collegate, seleziona le regioni da cui aggregare i dati.
8. Selezionare Salva.

Revisione delle impostazioni di aggregazione tra regioni

È possibile visualizzare l'attuale configurazione di aggregazione interregionale in AWS Security Hub da qualsiasi AWS regione nell'account amministratore o in un account autonomo. Gli account dei

membri non possono visualizzare la configurazione di aggregazione tra regioni. La configurazione include la regione principale e le regioni collegate (se presenti).

Segui i passaggi per visualizzare le impostazioni correnti di aggregazione tra le regioni

Per visualizzare le impostazioni di aggregazione tra regioni (console)

1. Apri la console AWS Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Nel pannello di navigazione, scegli Impostazioni e poi Generale.
3. Se l'aggregazione tra regioni non è abilitata, nella pagina Generale viene visualizzata l'opzione per abilitare l'aggregazione tra regioni. Solo gli account amministratore e gli account autonomi possono abilitare l'aggregazione tra aree geografiche.
4. Se l'aggregazione tra regioni è abilitata, la scheda Regioni visualizza le seguenti informazioni:
   - La regione di origine
   - Se aggregare automaticamente risultati, risorse e tendenze provenienti da nuove regioni supportate da Security Hub e per le quali hai scelto di aderire
   - L'elenco delle regioni collegate (se selezionate)

Aggiornamento delle impostazioni di aggregazione tra regioni

Puoi aggiornare le tue attuali impostazioni di aggregazione interregionale in AWS Security Hub modificando le Regioni collegate o la regione principale corrente.

Le modifiche all'aggregazione tra aree geografiche non vengono implementate per una regione attiva finché non abiliti la regione nel tuo account. AWS Le regioni AWS introdotte a partire dal 20 marzo 2019 sono regioni che hanno aderito all'iniziativa.

Quando si interrompe l'aggregazione dei dati da una regione collegata, AWS Security Hub non rimuove alcun dato aggregato esistente da quella regione accessibile nella regione di origine.

Non è possibile utilizzare le procedure di aggiornamento in questa sezione per modificare la regione di origine. Per cambiare la regione d'origine, devi fare quanto segue:

1. Elimina l'attuale configurazione di aggregazione tra regioni. Per istruzioni, consulta l'argomento the section called "Eliminazione dell'aggregazione".
2. Passa alla regione che desideri utilizzare come nuova regione di origine.

3. Abilita l'aggregazione tra regioni. Per istruzioni, consulta l'argomento the section called "Abilitare l'aggregazione".

È necessario aggiornare la configurazione di aggregazione tra regioni dalla regione principale corrente.

Per modificare le regioni collegate (console)

1. Dall'account amministratore o in un account autonomo, apri la console AWS Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Accedi alla regione di aggregazione corrente.
3. Nel menu di navigazione di Security Hub, scegli Impostazioni, quindi scegli Generale.
4. Per l'Cross-Region aggregazione, scegli Modifica.
5. Per le regioni collegate, aggiorna le aree collegate selezionate.
6. Selezionare Salva.

Eliminazione dell'aggregazione tra regioni

Se non desideri che AWS Security Hub aggreghi i dati, puoi eliminare il tuo aggregatore di risultati. In alternativa, puoi mantenere l'aggregatore di risultati ma non collegare alcuna regione alla AWS regione d'origine aggiornando l'aggregatore esistente in modo che non abbia selezionato alcuna regione collegata.

Per cambiare la tua regione di residenza, devi eliminare l'attuale aggregatore di risultati e crearne uno nuovo.

Quando elimini il tuo aggregatore di risultati, Security Hub interrompe l'aggregazione dei dati. Non rimuove alcun dato aggregato esistente dalla regione di origine.

Eliminazione dell'aggregatore di ricerca (console)

Puoi eliminare l'aggregatore di risultati solo dalla regione di residenza corrente.

Nelle regioni diverse dalla regione di origine, il pannello di aggregazione Finding sulla console Security Hub visualizza un messaggio che indica che è necessario modificare la configurazione nella regione di origine. Scegli questo messaggio per visualizzare un collegamento per passare alla regione d'origine.

Per interrompere l'aggregazione tra regioni (console)

1. Apri la console AWS Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Assicurati di aver effettuato l'accesso alla tua regione di residenza attuale.
3. Nel menu di navigazione di Security Hub, scegli Impostazioni, quindi scegli Generale.
4. In Cross-Region aggregazione, scegli Modifica.
5. In Regione di aggregazione, scegli Nessuna regione di aggregazione.
6. Selezionare Salva.
7. Nella finestra di dialogo di conferma, nel campo di conferma, digita. **`Confirm`**
8. Scegli Conferma.

Integrazione di Security Hub con Microsoft Azure

Per monitorare le tue risorse Microsoft Azure, puoi integrare Microsoft Azure con Security Hub. AWS Security Hub abilita quindi automaticamente la gestione della postura e delle vulnerabilità per il tuo ambiente Azure e genera risultati e altri dati sull'ambiente. Non è necessario attivare alcun servizio di sicurezza di Azure: tutte le funzionalità vengono eseguite da. AWS Più specificamente, il servizio offre quanto segue:

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

Verifiche di conformità automatizzate rispetto allo standard CIS Azure v4.0 e allo standard Azure Foundational Best Practices. Questi standard riguardano i controlli di identità, rete, archiviazione, registrazione e database.

Gestione della vulnerabilità

Amazon Inspector esegue automaticamente la scansione delle tue VM di Azure, delle Function Apps e delle immagini dei container di Azure Container Registry (ACR) alla ricerca di vulnerabilità software tramite il connettore collegato al servizio.

> **Note**
>
> La scansione delle macchine virtuali richiede che Amazon EC2 Systems Manager sia configurato nella stessa regione. Per i dettagli sulla configurazione, consulta la documentazione di Amazon Inspector per l'integrazione con Azure.

Correlazione dell'esposizione

Rilevamento automatico delle risorse di Azure esposte in base alla raggiungibilità della rete, all'accesso pubblico e alle combinazioni di errori di configurazione.

Avvisi di rilevamento delle minacce di Microsoft Defender for Cloud

Se configuri l'esportazione continua di Azure Defender nell'Event Hub, Security Hub acquisisce gli avvisi di rilevamento delle minacce di Defender for Cloud e li mappa nel formato Open Cybersecurity Schema Framework (OCSF). Questi vengono visualizzati insieme alla gestione della postura e ai risultati delle vulnerabilità nella console di Security Hub.

Inventario delle risorse

Un inventario completo delle risorse di Azure scoperte tramite l'integrazione, visibile nella console di Security Hub insieme alle tue AWS risorse.

Formato OCSF

Security Hub genera tutti i risultati nel formato Open Cybersecurity Schema Framework (OCSF), fornendo uno schema coerente tra i risultati di Azure. AWS

Per creare l'integrazione, connetti il tuo ambiente Azure a Security Hub tramite la seguente procedura:

1. Si configura l'ambiente Azure con una registrazione dell'applicazione, credenziali di identità federate, assegnazioni di ruolo di Azure e infrastruttura Event Hub.
2. Utilizzando la console Security Hub, crei un connettore per l'integrazione. Specifichi l'ID del tenant di Azure, l'ID del client dell'applicazione, l'ambito di monitoraggio e l'area Event Hub.
3. Security Hub crea i ruoli e le risorse necessari collegati ai servizi nel tuo. Account AWS
4. AWS Config raccoglie i dati di configurazione delle risorse dal tuo ambiente Azure.

   AWS Config viene utilizzato internamente per raccogliere i dati di configurazione delle risorse. A differenza della gestione della AWS postura, in cui è necessario abilitare AWS Config e pagare esplicitamente la registrazione, la gestione della postura di Azure viene gestita automaticamente. AWS Config Non è necessario abilitare AWS Config separatamente, configurare un registratore o pagare separatamente per l'utilizzo. AWS Config Questi costi sono inclusi nel prezzo di Security Hub.
5. Security Hub inizia a ricevere i dati di configurazione delle risorse e gli eventi del registro delle attività dall'ambiente Azure.

6. Security Hub genera la gestione della postura e i risultati delle vulnerabilità sull'ambiente Azure.

In che modo AWS Config viene utilizzato

AWS Config viene utilizzato internamente per raccogliere i dati di configurazione delle risorse e rilevare le modifiche nell'ambiente Azure. Il connettore lo gestisce automaticamente. Non è necessario abilitarlo AWS Config separatamente, configurare un registratore o pagare per AWS Config l'utilizzo. Questi costi sono inclusi nei prezzi del Security Hub per le risorse di Azure.

Informazioni aggiuntive

Quando crei l'integrazione, Security Hub crea automaticamente anche le corrispondenti integrazioni collegate ai servizi in Security Hub CSPM e Amazon Inspector. Queste integrazioni collegate ai servizi assicurano che l'ambito dei controlli CSPM e delle scansioni delle vulnerabilità di Inspector corrisponda all'ambito definito in Security Hub. Se desideri modificare l'ambito, devi apportare le modifiche nel Security Hub. Non è possibile modificare un'integrazione collegata ai servizi direttamente in Security Hub CSPM o Inspector.

Puoi anche creare un'integrazione di Azure direttamente in Security Hub CSPM e specificare impostazioni di ambito indipendenti. L'integrazione CSPM opera quindi indipendentemente dall'integrazione di Security Hub e può avere diversi ambiti di sottoscrizione di Azure e regione di Azure.

Per informazioni sulla stima e il calcolo dei costi per l'integrazione di Security Hub con Azure, vedi i prezzi di Security Hub. AWS

Argomenti

- Prerequisiti per l'integrazione di Security Hub con Microsoft Azure
- Configurazione di Microsoft Azure per l'integrazione con Security Hub
- Configurazione del Security Hub per l'integrazione con Microsoft Azure
- Eliminazione di un connettore Microsoft Azure in Security Hub

Prerequisiti per l'integrazione di Security Hub con Microsoft Azure

Prima di integrare Microsoft Azure con AWS Security Hub, completa le seguenti attività nel tuo ambiente AWS e in quello di Azure. Questo aiuta a garantire che tu e Security Hub disponiate delle risorse e delle autorizzazioni necessarie per monitorare le risorse di Azure.

Argomenti

- Prerequisiti per AWS
- Prerequisiti per Microsoft Azure

Prerequisiti per AWS

Verifica di avere quanto segue nel tuo Account AWS:

AWS Security Hub abilitato

Security Hub deve essere abilitato nel Account AWS Regione AWS punto in cui si desidera creare il connettore. È necessario abilitare Security Hub prima di creare un connettore di Azure.

AWS Security Hub (CSPM) abilitato

Security Hub CSPM deve essere abilitato nello stesso e. Account AWS Regione AWS L'integrazione con Azure si basa su Security Hub CSPM per la valutazione della configurazione delle risorse.

Autorizzazioni IAM della console

Il responsabile IAM che crea il connettore deve disporre delle seguenti autorizzazioni:

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

IAM Outbound Identity Federation è abilitata

Devi abilitare IAM Outbound Identity Federation nel tuo. Account AWS Questa funzionalità consente ai AWS servizi di autenticarsi con provider di identità esterni (come Microsoft Entra ID) utilizzando credenziali federate anziché segreti di lunga durata.

Dopo aver abilitato Outbound Identity Federation, annota l'URL dell'emittente del token. Questo URL segue il formato:

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

Questo URL ti servirà per configurare le credenziali di identità federate in Azure.

Prerequisiti per Microsoft Azure

Verifica di avere quanto segue nel tuo ambiente Azure:

Tenant di Azure

Devi avere un tenant di Azure nel cloud commerciale di Azure. Azure Government e Azure China non sono supportati.

Disponibilità del registro Microsoft Entra ID

La registrazione delle risorse richiede i registri di controllo e i registri di accesso di Microsoft Graph dal tenant dell'ID Microsoft Entra. Alcuni registri Microsoft Entra ID richiedono una licenza Microsoft Entra ID P1 o P2.

Se il tenant non dispone dei registri richiesti, la registrazione delle risorse potrebbe segnalare errori parziali. La registrazione dell'app e le assegnazioni dei ruoli di Azure non forniscono dati di registro mancanti.

Ruolo di amministratore globale

È necessario disporre del ruolo di amministratore globale in Microsoft Entra ID per configurare l'ambiente Azure. Questo ruolo è necessario per registrare le applicazioni, concedere il consenso dell'amministratore per le autorizzazioni dell'API Microsoft Graph, assegnare ruoli RBAC nell'ambito del gruppo di gestione principale del tenant e configurare le impostazioni diagnostiche per Entra ID Audit Logs.

Oltre a Global Administrator, sono necessari i seguenti ruoli Azure RBAC per creare le risorse richieste dall'integrazione:

- User Access Administrator (o Owner) nell'ambito principale (`/`): per assegnare i ruoli RBAC nell'ambito del gruppo di gestione principale del tenant.
- Resource Policy Contributor (o Owner) nell'ambito del gruppo di gestione principale del tenant, per creare le definizioni e le assegnazioni delle Azure Policy che automatizzano le impostazioni diagnostiche e la correzione.
- Collaboratore (o proprietario) nell'ambito della sottoscrizione che ospita l'Event Hub, per creare lo spazio dei nomi Event Hub e le risorse correlate.

> **Note**
>
> In molte organizzazioni, l'amministratore globale di Azure e l'amministratore della AWS sicurezza sono persone diverse. La configurazione di Azure può essere completata in modo indipendente utilizzando lo script di configurazione generato.

Dopo aver completato queste attività, sei pronto per configurare il tuo ambiente Azure.

Configurazione di Microsoft Azure per l'integrazione con Security Hub

Dopo aver completato le attività relative ai prerequisiti, puoi configurare il tuo ambiente Microsoft Azure per supportare l'integrazione con AWS Security Hub. Per aiutarti a farlo, la console Security Hub genera uno script di configurazione personalizzato per la tua configurazione.

Per generare lo script di configurazione

1. Aprire la console AWS Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/advanced/home? region=us-east-1. .
2. Nel riquadro di navigazione, scegli Integrazioni.
3. Scegli Crea connettore Azure.
4. Completa la configurazione del connettore (ID del tenant, ambito e nome), quindi copia lo script di configurazione generato.

Per eseguire lo script, usa l'interfaccia della riga di comando di Azure ed esegui l'autenticazione con un account Global Administrator (). `az login`

Quando esegui lo script, esegue una serie di attività. Le sezioni seguenti descrivono ogni operazione eseguita dallo script. Se l'organizzazione limita l'esecuzione degli script, è possibile eseguire queste attività manualmente, utilizzando questo argomento come guida. Dopo aver configurato l'ambiente Azure, puoi configurare Security Hub per l'integrazione con Azure.

I passaggi 1—7 configurano la base condivisa utilizzata da tutte le funzionalità di Security Hub: registrazione dell'applicazione, credenziali federate, assegnazioni di ruolo di Azure, autorizzazioni Microsoft Graph, Event Hub ed esportazione dei log. I passaggi 8-10 configurano le risorse aggiuntive di Azure per funzionalità specifiche:

- Gestione delle vulnerabilità (Amazon Inspector): configura l'esportazione degli eventi del repository di Azure Container Registry (ACR) e un'identità gestita assegnata dal sistema sulle tue macchine virtuali di Azure.
- Rilevamento delle minacce (Microsoft Defender for Cloud): configura Microsoft Defender for Cloud per esportare continuamente gli avvisi di sicurezza nell'Event Hub.

> **Note**
>
> Una singola registrazione dell'app di Azure è condivisa tra i servizi di sicurezza. AWS Se usi anche Security Hub CSPM o Amazon Inspector for Azure, utilizzano la stessa registrazione dell'app. Non è necessario creare registrazioni separate per ogni servizio. AWS

Processi

- Passaggio 1: registrare un'applicazione Azure
- Fase 2: Creare un'entità del servizio
- Passaggio 3: configurare le credenziali di identità federate
- Fase 4: Assegnazione dei ruoli RBAC
- Passaggio 5: configurare le autorizzazioni dell'API Microsoft Graph
- Passaggio 6: configura Azure Event Hub
- Fase 7: Configurazione dell'esportazione del registro delle attività e del registro di controllo Entra ID
- Passaggio 8: configurare l'esportazione del registro di Azure Container
- Passaggio 9: abilitare un'identità gestita sulle macchine virtuali di Azure
- Passaggio 10: esporta gli avvisi di Microsoft Defender for Cloud

Passaggio 1: registrare un'applicazione Azure

Registra una nuova applicazione in Microsoft Entra ID. Questa applicazione funge da identità AWS utilizzata per l'autenticazione nell'ambiente Azure utilizzando credenziali federate. Non sono richiesti i segreti del cliente.

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

Annota l'ID dell'applicazione (client) dall'output (l'`appId`attributo). Questo valore verrà fornito durante la creazione del connettore nella console Security Hub.

Fase 2: Creare un'entità del servizio

Creare un'entità di servizio per l'applicazione registrata. Si utilizzano le assegnazioni di ruolo di Azure per concedere le autorizzazioni all'entità del servizio. Il responsabile del servizio esegue azioni nel tuo ambiente Azure.

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

*`application-client-id`*Dov'è l'ID dell'applicazione (client) del passaggio precedente.

Imposta l'URI dell'ID dell'applicazione sulla registrazione su`api://`*`application-client-id`*. AWS richiede questo identificatore per scambiare token federati con l'applicazione. Senza questo URI, AWS non è possibile produrre un pubblico di token federati valido e ogni funzionalità non riesce ad autenticarsi in Azure.

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

Passaggio 3: configurare le credenziali di identità federate

Configurare le credenziali di identità federate sull'applicazione per consentire l'autenticazione senza segreti del AWS cliente. Questo stabilisce un trust OIDC tra Azure e Azure. AWS Non vengono archiviati segreti o credenziali di lunga durata.

L'integrazione di Security Hub Azure esegue l'autenticazione utilizzando un ruolo AWS IAM per funzionalità: rilevamento della configurazione delle risorse, gestione delle vulnerabilità e rilevamento delle minacce. Aggiungi una credenziale di identità federata per ogni ruolo in modo che ogni funzionalità possa autenticarsi in Azure. AWS crea automaticamente i ruoli collegati al servizio quando si crea il connettore. Il ruolo `Inspector2SSMFederationRole` utilizzato per la scansione delle VM non è un ruolo collegato ai servizi; lo crei come parte della configurazione della scansione delle macchine virtuali di Amazon Inspector, descritta nel passaggio 9. ???

Funzionalità	Oggetto (ruolo IAM ARN)
Individuazione della configurazione delle risorse ()AWS Config	`arn:aws:iam:: account-id :role/aws-service-role/thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty`
Gestione delle vulnerabilità (Inspector)	`arn:aws:iam:: account-id :role/aws-service-role/thirdparty.inspector2.amazonaws.com/AWSServiceRoleForAmazonInspector2ThirdParty`
Gestione delle vulnerabilità: scansione delle macchine virtuali (Amazon EC2 Systems Manager)	`arn:aws:iam:: account-id :role/Inspector2SSMFederationRole- tenant-id`
Rilevamento delle minacce (Security Hub)	`arn:aws:iam:: account-id :role/aws-service-role/securityhubv2.amazonaws.com/AWSServiceRoleForSecurityHubV2`

Esegui il comando seguente una volta per ogni oggetto della tabella precedente, modificando ogni volta `subject` i valori `name` e. I `audiences` valori `issuer` e sono gli stessi per tutte le credenziali.

```
$ 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"
  }'
```

Valori chiave:

- Emittente: l'URL dell'emittente del token fornito da IAM Outbound Identity Federation. Segue il formato. `https://uuid.tokens.sts.global.api.aws`

- Oggetto: un ARN del ruolo IAM riportato nella tabella precedente. Il ruolo *`tenant-id`* di Amazon EC2 Systems Manager è il tuo ID tenant di Azure.
- Destinatari: `api://AzureADTokenExchange` (valore standard per la federazione delle identità dei carichi di lavoro).
- Nome: qualsiasi nome univoco all'interno dell'applicazione.

Fase 4: Assegnazione dei ruoli RBAC

Assegna i seguenti ruoli integrati al responsabile del servizio:

- Reader: concede l'accesso in sola lettura a tutte le risorse di Azure, in modo che Security Hub possa scoprire e valutare le configurazioni delle risorse. Assegna questo ruolo nell'ambito principale (). `/`
- Collaboratore: concede l'accesso in scrittura richiesto da Amazon Inspector per scansionare le tue macchine virtuali di Azure, le Function Apps e le immagini dei container alla ricerca di vulnerabilità. Assegna questo ruolo nell'ambito del gruppo di gestione principale del tenant, che lo propaga a tutte le sottoscrizioni del tenant.
- Ricevitore dati di Azure Event Hub: consente di AWS leggere gli eventi dall'Event Hub. Assegna questo ruolo nell'ambito del gruppo di gestione principale del tenant.

⚠ Assegna Reader all'ambito principale

Assicuratevi di assegnare il ruolo Reader nell'ambito principale (`/`), non nell'ambito del gruppo di gestione principale del tenant. Security Hub legge le risorse di Azure per l'assegnazione dei ruoli in ogni ambito, incluse le assegnazioni con ambito nella radice del tenant. Un'assegnazione Reader nel gruppo di gestione principale non copre le assegnazioni il cui ambito è`/`, quindi senza di essa tali letture hanno esito negativo con un errore di autorizzazione e il connettore può entrare in uno stato degradato.

⚠ Il collaboratore concede l'accesso in scrittura a livello di tenant

Il ruolo di collaboratore nell'ambito del gruppo di gestione principale dei tenant concede un accesso in scrittura altamente privilegiato a livello di tenant alle risorse di Azure. Security Hub richiede questo accesso in modo che Amazon Inspector possa scansionare le tue risorse di calcolo alla ricerca di vulnerabilità. Ad esempio, Inspector utilizza le autorizzazioni di

esecuzione dei comandi della macchina virtuale fornite da Contributor. Tramite Amazon EC2 Systems Manager Automation, Inspector esegue comandi sulle macchine virtuali di Azure per installare e utilizzare l'agente VM Scanner.

```
$ 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 l'assegnazione richiede un accesso elevato

L'assegnazione di un ruolo nell'ambito principale (/) richiede un accesso elevato. Se l'assegnazione di un ruolo non riesce, verifica che la gestione degli accessi per le risorse di Azure sia impostata su Sì in Microsoft Entra ID > Proprietà. Quindi esci e accedi nuovamente per aggiornare il token.

Rimuovi l'elevazione temporanea della radice

L'abilitazione della gestione degli accessi per le risorse di Azure concede all'amministratore che ha effettuato l'accesso il ruolo di amministratore dell'accesso utente nell'ambito principale (/), che può gestire l'accesso in ogni sottoscrizione e gruppo di gestione del tenant. Una volta completato l'onboarding, imposta la gestione degli accessi per le risorse di Azure su No in Microsoft Entra ID > Proprietà, salva ed esci in modo che questa elevazione non rimanga attiva.

Passaggio 5: configurare le autorizzazioni dell'API Microsoft Graph

Concedi le seguenti autorizzazioni API Microsoft Graph (tipo di applicazione) all'applicazione, quindi concedi il consenso dell'amministratore:

- `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
```

Passaggio 6: configura Azure Event Hub

AWS Config utilizza un Azure Event Hub per ricevere notifiche quasi in tempo reale sulle modifiche alla configurazione delle risorse nel tuo ambiente Azure. Lo script di configurazione crea l'infrastruttura Event Hub e la contrassegna per l'individuazione. Event Hub discovery utilizza una risoluzione basata su tag: Security Hub cerca un tag nel namespace di Event Hub con il formato `AWSConfig-account-id-region` per identificare l'istanza di Event Hub corretta per la tua integrazione.

```
$ 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"
```

Dopo aver creato l'Event Hub, contrassegna il namespace per il rilevamento e assegna il ruolo di Ricevitore dati. Usa `az tag update` with `--operation merge` in modo da preservare tutti gli altri tag presenti nel namespace (ad esempio il tag di rilevamento delle minacce riportato nella Fase 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**
>
> Nel formato tag`AWSConfig-account-id-region`, *`account-id`* è il tuo Account AWS ID a 12 cifre ed *`region`* è il Regione AWS luogo in cui stai creando il connettore (ad esempio,). `us-east-1` Questi valori identificano a quale regione Account AWS appartiene questa integrazione Event Hub.

Configurazione chiave:

- Namespace SKU: standard (obbligatorio per i gruppi di consumatori).
- Nome Event Hub —. `activitylog`
- Gruppo di consumatori —`AWSConfig`.
- Etichetta: `AWSConfig-`*`account-id`*`-`*`region`* con valore`activitylog`. Questo tag consente di AWS Config scoprire automaticamente l'Event Hub.
- Assegnazione dei ruoli: ricevitore dati di Azure Event Hub nel namespace.

Per il rilevamento delle minacce, la configurazione crea anche un `defender-alerts` Event Hub separato con un gruppo di `AWSSecurityHub` consumatori e aggiunge un secondo tag di rilevamento nel formato `AWSSecurityHub-`*`account-id`*`-`*`region`* che identifica gli hub letti direttamente da Security Hub. Per ulteriori informazioni, consulta il passaggio 10.

Fase 7: Configurazione dell'esportazione del registro delle attività e del registro di controllo Entra ID

Configura Azure per esportare i registri delle attività e i registri degli ID Microsoft Entra nell'Event Hub.

Esportazione del registro delle attività:

Configura le impostazioni diagnostiche su ogni abbonamento per esportare i registri delle attività nell'Event Hub. Lo script di configurazione lo configura automaticamente per tutti gli abbonamenti monitorati. I registri delle attività registrano le attività a livello di abbonamento, comprese le assegnazioni di ruolo e le modifiche alle risorse.

Esportazione del registro ID Microsoft Entra:

Configura le impostazioni diagnostiche sull'ID Microsoft Entra per esportare i registri nello stesso Event Hub. Accedere a Microsoft Entra ID > Monitoraggio > Impostazioni diagnostiche > Aggiungi impostazioni di diagnostica. Abilita AuditLogs SignInLogs NonInteractiveUserSignInLogs, e indirizzali al tuo Event Hub.

Passaggio 8: configurare l'esportazione del registro di Azure Container

Security Hub analizza le immagini del contenitore Azure Container Registry (ACR) per individuare eventuali vulnerabilità tramite Amazon Inspector. Per fare ciò, Inspector ha bisogno che gli eventi del repository ACR siano esportati in un Event Hub nella stessa regione di Azure del registro. Per la configurazione dell'esportazione ACR, consulta Configurazione di Amazon Inspector per l'integrazione con Microsoft Azure nella Amazon Inspector User Guide.

Passaggio 9: abilitare un'identità gestita sulle macchine virtuali di Azure

Security Hub esegue la scansione delle macchine virtuali di Azure tramite Inspector. Ogni macchina virtuale di Azure di destinazione deve avere un'identità gestita assegnata dal sistema abilitata. Per aggiungere automaticamente questa identità alle tue macchine virtuali, assegna due policy di Azure che utilizzano l'`modify`effetto nell'ambito del gruppo di gestione principale del tenant:

- Per una macchina virtuale senza identità, la policy aggiunge un'identità gestita assegnata dal sistema.
- Per una macchina virtuale che ha solo un'identità assegnata dall'utente, la policy aggiunge un'identità gestita assegnata dal sistema preservando le identità esistenti assegnate dall'utente.

Una macchina virtuale che ha già un'identità gestita assegnata dal sistema rimane invariata. Poiché le policy utilizzano l'`modify`effetto, regolano l'identità senza ridistribuire la VM.

Inspector utilizza Amazon EC2 Systems Manager Automation per distribuire e gestire l'agente Inspector VM Scanner sulle tue macchine virtuali di Azure. Ciò richiede una configurazione aggiuntiva, tra cui un AWS provider di identità IAM OIDC per Microsoft Entra ID e diversi ruoli IAM. Per la configurazione completa della scansione delle macchine virtuali, consulta Configurazione di Amazon Inspector per l'integrazione con Microsoft Azure nella Amazon Inspector User Guide.

Passaggio 10: esporta gli avvisi di Microsoft Defender for Cloud

Security Hub acquisisce gli avvisi di rilevamento delle minacce di Microsoft Defender for Cloud e li mappa nel formato Open Cybersecurity Schema Framework (OCSF). Per fornire questi avvisi, crea un `defender-alerts` Event Hub dedicato e configura Microsoft Defender for Cloud per esportare continuamente gli avvisi di sicurezza al suo interno.

Nello spazio dei nomi Event Hub del passaggio 6, crea `defender-alerts` Event Hub, un gruppo di `AWSSecurityHub` consumatori da cui Security Hub può leggere e una regola di autorizzazione SAS (Shared Access Signature) con ambito hub con autorizzazione di invio che Microsoft Defender for Cloud utilizza per inviare avvisi:

```
$ 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
```

Quindi, unisci un secondo tag di scoperta nel namespace in modo che Security Hub scopra l'hub. `defender-alerts` Usalo `az tag update` con `--operation merge` in modo da conservare il tag di `AWSConfig` scoperta del passaggio 6: ???

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

Infine, configura l'esportazione continua da Microsoft Defender for Cloud del tipo di dati degli avvisi di sicurezza nell'`defender-alerts`Event Hub. Nel portale di Azure, vai a Microsoft Defender for Cloud > Impostazioni ambiente, seleziona l'abbonamento, scegli Esportazione continua > Event Hub, seleziona Avvisi di sicurezza e scegli `defender-alerts` Event Hub e la regola SAS. `DefenderExportSend`

> **Note**
>
> Se configuri l'esportazione continua a livello di codice (tramite l'API Azure Resource Manager, un modello ARM o Azure Policy) anziché nel portale, autentica l'esportazione nell'Event Hub con la stringa di connessione SAS. `DefenderExportSend` Recuperatelo con `az eventhubs eventhub authorization-rule keys list` la `DefenderExportSend` regola e impostatelo come stringa di connessione dell'azione di esportazione. Per ulteriori informazioni, vedi Configurare l'esportazione continua nella documentazione di Microsoft Azure.

> **Note**
>
> Dopo aver completato queste attività, attendi circa 15-30 minuti affinché la configurazione abbia effetto. Quindi, verifica che il tuo Event Hub riceva messaggi (la IncomingMessages metrica) prima di creare il connettore in Security Hub.

Configurazione del Security Hub per l'integrazione con Microsoft Azure

Dopo aver completato le attività preliminari e configurato l'ambiente Microsoft Azure, puoi configurare AWS Security Hub per l'integrazione con Azure. Per configurare Security Hub per l'integrazione con Azure, devi creare un connettore. È possibile creare il connettore da un account amministratore delegato o dall'account di gestione. Dopo aver creato il connettore, si verificano i seguenti eventi:

1. Security Hub convalida le credenziali e la connettività di Azure all'ambiente Azure. Questo processo può richiedere alcuni minuti.
2. Security Hub crea connettori collegati ai servizi in Security Hub CSPM e Amazon Inspector. Questi connettori assicurano che i controlli di gestione della postura e la scansione delle vulnerabilità corrispondano all'ambito definito in Security Hub.
3. AWS Config inizia a scoprire le risorse di Azure usando le credenziali di identità federate.
4. Security Hub abilita automaticamente lo standard CIS Microsoft Azure Foundations Benchmark v4.0 e lo standard Azure Foundational Best Practices in CSPM per le risorse di Azure.
5. I risultati iniziali iniziano a comparire entro 15-30 minuti per le risorse con eventi Activity Log. La valutazione completa di tutte le risorse esistenti può richiedere fino a 24 ore.

Argomenti

- Crea un connettore Azure
- Modifica l'ambito di un connettore Azure
- Verifica lo stato di un connettore di Azure
- Risolvi i problemi relativi a un connettore Azure
- In che modo Security Hub gestisce le risorse e gli identificatori di ricerca

Crea un connettore Azure

Per creare un connettore Microsoft Azure per il tuo ambiente, completa i passaggi seguenti utilizzando la console AWS Security Hub o l'API.

1. Aprire la console AWS Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/advanced/home? region=us-east-1. .
2. Nel riquadro di navigazione, scegli Integrazioni.
3. Scegli Crea connettore Azure.
4. Nella sezione Funzionalità di sicurezza, scegli se desideri abilitare la funzionalità di scansione della rete. Questa funzionalità è abilitata per impostazione predefinita per l'account in cui stai abilitando l'integrazione con Azure e può essere deselezionata prima di completare la configurazione del connettore. Se una politica dell'organizzazione blocca questa funzionalità per il tuo account, questa non viene visualizzata come opzione. Per ulteriori informazioni, vedere Scansione della rete in Security Hub.
5. Per Azure Tenant ID, inserisci l'identificatore del tenant ID Microsoft Entra. Puoi trovarlo nel portale di Azure in Microsoft Entra ID > Proprietà > ID tenant.
6. Per l'ID dell'applicazione (client), inserisci l'ID dell'applicazione Azure che hai registrato durante la configurazione dell'ambiente Azure.
7. Configura impostazioni aggiuntive e l'ambito del connettore effettuando le seguenti operazioni:

   - In Nome, inserisci un nome univoco per il connettore. Il nome può contenere fino a 50 caratteri alfanumerici e può includere trattini.

     > **Note**
     >
     > Il nome del connettore non può essere modificato dopo la creazione.

   - Per Descrizione, inserisci facoltativamente una breve descrizione del connettore. La descrizione può contenere fino a 200 caratteri.

   > **Important**
   >
   > I nomi e le descrizioni vengono utilizzati per identificare i contenuti. Non includete in essi informazioni sensibili, riservate o di identificazione personale (PII).

- Per Abbonamenti, scegli Tutti gli abbonamenti per monitorare tutti gli abbonamenti attuali e futuri nel tenant o Abbonamenti specifici per monitorare solo gli abbonamenti specificati. Se scegli di monitorare solo abbonamenti specifici, inserisci l'ID per ognuno di essi.
- Per Regioni, scegli Tutte le aree per monitorare le risorse in tutte le aree di Azure o Aree specifiche per monitorare solo le regioni specificate.

> **Note**
>
> Se hai già creato un connettore in Security Hub CSPM o Amazon Inspector per lo stesso tenant di Azure, l'ambito del connettore in Security Hub deve includere gli stessi abbonamenti e le stesse regioni del connettore in Security Hub CSPM o Amazon Inspector.

> **Note**
>
> I controlli che valutano le risorse Microsoft Entra ID e Microsoft Graph richiedono che l'ambito regionale globale sia incluso nella configurazione di integrazione. Se selezioni solo aree di Azure specifiche, questi controlli non generano risultati.

8. Esamina la configurazione del connettore.

> **Note**
>
> Se prevedi di utilizzare Amazon Inspector for Azure VM scanning, devi creare i ruoli IAM richiesti. Per informazioni dettagliate, vedi the section called "Ruoli IAM per la scansione delle macchine virtuali".

9. Quando hai finito di inserire e rivedere le impostazioni, scegli Crea connettore.

Ruoli IAM per la scansione delle macchine virtuali di Azure tramite Amazon Inspector

Per abilitare la scansione delle vulnerabilità tramite Amazon Inspector, devi creare le seguenti risorse IAM nel tuo. Account AWS

Provider di identità IAM OIDC

Crea un provider di identità IAM OIDC per Microsoft Entra ID con la seguente configurazione:

- URL dell'emittente: `https://sts.windows.net/`*`tenant-id`*`/`
- Elenco di ID client:`api://`*`app-id`*, `api://AzureADTokenExchange`
- Thumbprint: una stringa di 40 caratteri con tutti gli zeri (`0`ripetuta 40 volte). AWS STS convalida i token tramite l'endpoint JWKS anziché il valore dell'impronta digitale.

Inspector2VmScannerRole-***`tenant-id`***

Utilizzato dall'agente Amazon Inspector VM Scanner in esecuzione su macchine virtuali di Azure per inviare telemetria di scansione ad Amazon Inspector. Questo ruolo utilizza la federazione delle identità Web OIDC tramite il provider di identità. Microsoft Entra ID

Politica di fiducia:

```
{
    "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"
                }
            }
        }
    ]
}
```

Tag:

- `inspector-managed` = `true`

Politica di autorizzazione (TelemetryPolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "inspector2-telemetry:*",
            "Resource": "*"
        }
    ]
}
```

Inspector2SSMFederationRole-***tenant-id***

Abilita la federazione OIDC ad Azure per l'autenticazione sicura tra cloud. Questo ruolo viene assunto da AssumeRole and e DispatchRole da Amazon EC2 Systems Manager per ottenere token di identità Web per le operazioni di Azure.

Politica di fiducia:

```
{
    "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"
        }
    ]
}
```

Politica di autorizzazione (FederationPolicy):

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

Tag:

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

Inspector2SSMAssumeRole-*tenant-id*

Esegue Amazon EC2 Systems Manager Automation per integrare le macchine virtuali di Azure come istanze gestite. Questo ruolo crea e gestisce attivazioni ibride, trasferisce i ruoli ad Amazon EC2 Systems Manager e recupera i documenti di automazione.

Politica di fiducia:

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

Politica di autorizzazione (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": "*"
        }
    ]
}
```

Tag:

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

Inspector2SSMDispatchRole-***tenant-id***

Risolve gli obiettivi delle macchine virtuali di Azure e invia l'installazione dell'agente Amazon Inspector VM Scanner tramite Amazon EC2 Systems Manager Automation. Questo ruolo avvia le esecuzioni di automazione e le passa AssumeRole ad Amazon EC2 Systems Manager.

Politica di fiducia:

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

Politica di autorizzazione (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": "*"
        }
    ]
}
```

Tag:

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

Prerequisiti per la scansione delle VM

L'URI dell'ID dell'applicazione per la registrazione dell'app Azure deve essere impostato su. `api://app-id`

Ogni macchina virtuale di Azure che si desidera scansionare deve avere un'identità gestita assegnata dal sistema abilitata. Per assegnare automaticamente l'identità gestita alle nuove macchine virtuali, usa una DeployIfNotExists policy nel tuo ambiente Azure.

Dopo aver creato il connettore, Security Hub inizia a monitorare l'ambiente Azure. Puoi controllare lo stato del connettore nella pagina Integrazioni.

Modifica l'ambito di un connettore Azure

Dopo aver creato un connettore Microsoft Azure, puoi modificare l'ambito del connettore modificando le sottoscrizioni di Azure o le aree di Azure che monitora. Le modifiche all'ambito in genere hanno effetto entro 15-30 minuti per le risorse con eventi Activity Log. La valutazione completa delle sottoscrizioni di Azure appena aggiunte può richiedere fino a 24 ore.

Prima di modificare l'ambito di un connettore, tieni presente quanto segue:

- Quando modifichi l'ambito di un connettore in Security Hub, i connettori collegati ai servizi associati in Security Hub CSPM e Amazon Inspector vengono automaticamente aggiornati in base alla situazione.
- L'ambito di un connettore Security Hub non può mai essere inferiore a quello di qualsiasi connettore gestito dal cliente esistente in Security Hub CSPM o Amazon Inspector per lo stesso tenant di Azure.
- Se aggiungi una regione all'ambito del connettore, devi eseguire nuovamente lo script di configurazione per fornire l'infrastruttura Event Hub nella nuova regione. La configurazione esistente di Event Hub non è interessata.

Verifica lo stato di un connettore di Azure

Puoi controllare lo stato di un connettore Microsoft Azure in qualsiasi momento per confermare che Security Hub stia ricevendo dati dal tuo ambiente Azure.

Per verificare lo stato di un connettore

1. Aprire la console AWS Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/advanced/home? region=us-east-1. .
2. Nel riquadro di navigazione, scegli Integrazioni e seleziona il tuo connettore Azure.

3. Verifica che lo stato del connettore sia Attivo. Se il connettore mostra Attivo, la verifica è completa. Se mostra uno stato diverso, vedithe section called "Risolvi i problemi relativi a un connettore".
4. Passa a Findings e filtra `ResourceCloudProviders = Azure` per confermare che i risultati vengono generati per le tue risorse di Azure.
5. Controlla la pagina degli standard di sicurezza per confermare che lo standard CIS Azure v4.0 mostra i controlli con lo stato PASSED o FAILED (non tutti NO_DATA).

> **Note**
>
> Lo stato di salute del connettore alla fine è coerente. Quando si verifica un problema di autorizzazione o configurazione, lo stato del connettore passa rapidamente a Degradato con un messaggio utilizzabile. Tuttavia, dopo aver risolto il problema, lo stato può richiedere fino a 24 ore per tornare a Connesso.
>
> - Uno stato Degrado dopo una correzione recente non indica necessariamente la presenza di un problema in corso.
> - Per una visibilità in tempo reale degli errori di registrazione, controlla le CloudWatch metriche nel namespace.

Risolvi i problemi relativi a un connettore Azure

Se riscontri problemi con il connettore, consulta i seguenti problemi e risoluzioni comuni.

Lo stato del connettore non è integro

Questo problema si verifica in genere se le credenziali federate non sono configurate correttamente in Azure.

Per risolvere questo problema, verifica che l'URL dell'emittente del token e l'ARN dell'oggetto nelle credenziali federate di Azure corrispondano ai tuoi. Account AWS

Nessun risultato dopo 30 minuti

Questo problema può verificarsi se l'Event Hub non riceve i registri delle attività.

Per risolvere questo problema, verifica che le impostazioni di diagnostica siano configurate nelle sottoscrizioni di Azure e che lo spazio dei nomi Event Hub sia etichettato correttamente con. `AWSConfig-`*`account-id`*`-`*`region`*

Tutti i controlli mostrano NO_DATA

Questo problema può verificarsi se il connettore è disabilitato o se AWS Config non riesce a raggiungere l'ambiente Azure.

Per risolvere questo problema, verifica che il connettore sia abilitato e che il responsabile del servizio abbia il ruolo Reader nell'ambito del gruppo di gestione principale del tenant.

Impossibile registrare alcune risorse di Azure

L'errore può verificarsi per uno dei seguenti motivi:

- L'ambiente Azure non soddisfa i prerequisiti per la registrazione delle risorse.
- La registrazione dell'app non dispone del consenso dell'amministratore per le autorizzazioni dell'API Microsoft Graph.
- L'assegnazione del ruolo Reader non copre tutti gli ambiti richiesti.
- Il tenant Microsoft Entra ID non dispone dei dati di registro richiesti.

Per risolvere l'errore, procedi come segue:

1. Per confermare che l'ambiente soddisfa tutti i requisiti, consulta Prerequisiti per Microsoft Azure.
2. Verifica che la registrazione dell'app disponga delle autorizzazioni necessarie per l'API Microsoft Graph con il consenso dell'amministratore.
3. Verifica che il responsabile del servizio abbia il ruolo di lettore nell'ambito del gruppo di gestione principale del tenant.

I risultati vengono visualizzati solo per alcuni abbonamenti

Questo problema può verificarsi se l'esportazione di Activity Log non è configurata per tutti gli abbonamenti di Target.

Per risolvere questo problema, verifica che le impostazioni di diagnostica coprano tutti gli abbonamenti inclusi nell'ambito del connettore.

In che modo Security Hub gestisce le risorse e gli identificatori di ricerca

Abilitando l'integrazione di Azure per AWS Security Hub, gli identificatori di risorse e risultati di sicurezza di altri provider cloud vengono archiviati in AWS Config Security Hub e altri AWS servizi (se necessario) come metadati relativi alla gestione della configurazione delle risorse corrispondente e ai dati di sicurezza raccolti dagli altri provider cloud. Tali identificatori non costituiscono i Contenuti dell'utente. Non includete in essi informazioni sensibili, riservate o che consentano l'identificazione personale.

I seguenti identificatori del tuo ambiente cloud connesso vengono archiviati e utilizzati da per AWS fornire funzionalità di sicurezza multicloud:

- Identificatori di risorse: Azure Tenant ID, ID di sottoscrizione, posizione (regione), ID risorsa (ID o nomi dei gruppi di risorse, provider di risorse, tipo di risorsa)
- Identificatori di sicurezza: gli identificatori univoci assegnati a ciascun risultato di sicurezza generato dal servizio di rilevamento.

Le relazioni tra questi identificatori, tra cui il modo in cui le risorse si relazionano tra loro e il modo in cui i risultati si relazionano alle risorse, vengono archiviate anche come metadati di servizio. AWS utilizza questi identificatori per la correlazione delle risorse, l'associazione dei risultati alle risorse, la registrazione operativa del servizio e la deduplicazione.

Eliminazione di un connettore Microsoft Azure in Security Hub

Dopo aver creato un connettore Microsoft Azure in AWS Security Hub, puoi eliminarlo in qualsiasi momento. Se elimini un connettore, Security Hub interrompe l'esecuzione dei controlli di gestione della postura e del monitoraggio delle vulnerabilità per l'ambiente Azure. Security Hub interrompe inoltre la generazione di nuovi risultati e altri dati sull'ambiente. I risultati esistenti vengono conservati per 90 giorni. L'inventario delle risorse rimane invariato al momento dell'eliminazione del connettore e viene rimosso dopo 90 giorni.

Quando elimini un connettore, Security Hub elimina automaticamente i connettori collegati ai servizi associati in AWS Security Hub CSPM e Amazon Inspector. Security Hub non elimina la registrazione delle applicazioni di Azure e l'infrastruttura Event Hub nel tuo ambiente Azure. È necessario eliminarli manualmente, direttamente in Microsoft Azure. Per informazioni su come, vedi Rimuovere un'applicazione nella documentazione di Microsoft Azure.

Per eliminare un connettore di Azure

1. Aprire la console AWS di Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/advanced/home? region=us-east-1. .
2. Nel riquadro di navigazione, scegli Integrazioni.
3. Seleziona il connettore che desideri eliminare.
4. Scegli Elimina.
5. Quando richiesto, conferma di voler eliminare il connettore.

> **Important**
>
> Se elimini un connettore e ne crei uno nuovo entro 6 ore, il rilevamento delle risorse potrebbe richiedere fino a 6 ore. Pianifica l'eliminazione e la ricreazione del connettore di conseguenza.

Utilizzo della dashboard di riepilogo in Security Hub

La dashboard di riepilogo nella console Security Hub mostra una panoramica delle esposizioni, delle minacce, delle risorse e della copertura di sicurezza tra i widget di sicurezza. Puoi personalizzare la dashboard aggiungendo e rimuovendo widget e creando e applicando set di filtri per recuperare i dati in ogni widget.

Considerazioni

Prima di interagire con la dashboard, considera quanto segue:

- Le personalizzazioni, come i set di filtri salvati o le modifiche al layout dei widget, vengono salvate automaticamente.
- I dati si aggiornano automaticamente ogni volta che apri la dashboard.
- Se configuri l'aggregazione tra regioni, la dashboard include i risultati di tutte le regioni collegate (quando si visualizza la dashboard nella regione principale).

Considera quanto segue se il tuo account è un account amministratore delegato per un'organizzazione, un account membro di un'organizzazione o un account autonomo.

- Le personalizzazioni effettuate da un account amministratore delegato verranno salvate indipendentemente dalle personalizzazioni effettuate dagli account dei membri. Le personalizzazioni possono includere set di filtri salvati o modifiche al layout dei widget.
- Se il tuo account è l'account amministratore delegato di un'organizzazione, i dati includono i risultati relativi al tuo account e agli account dei membri.
- Se il tuo account è un account membro di un'organizzazione o un account autonomo, i dati includono i risultati solo per il tuo account.

È consigliabile non includere informazioni riservate, sensibili o di identificazione personale (PII) nei set di filtri salvati, nei widget personalizzati o in altri campi di testo in formato libero correlati.

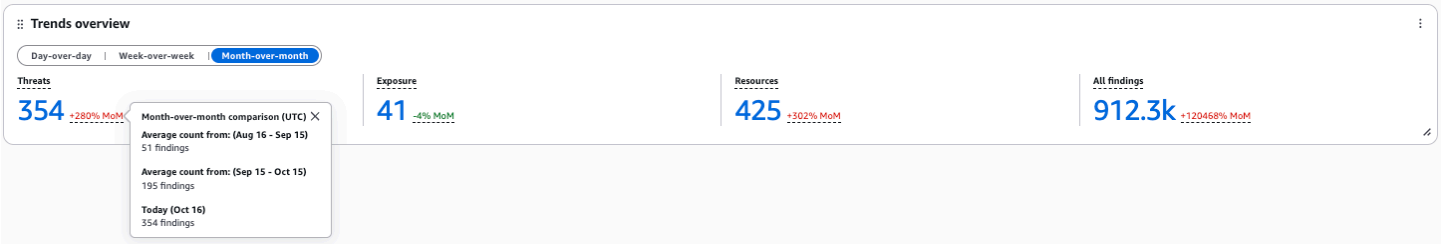
Widget disponibili

Puoi interagire con diversi widget nelle schede Executive e Triage della dashboard di riepilogo. La scheda Executive include widget che mostrano i dati sulle tendenze relative a esposizioni, minacce e risorse e il widget Security Coverage per aiutarti a monitorare la copertura del tuo account attraverso diverse funzionalità di sicurezza. La scheda Triage include widget che mostrano un riepilogo delle tue esposizioni, minacce e risorse. Tuttavia, puoi aggiungere widget, rimuovere widget e gestire la posizione di ciascun widget in entrambe le schede per personalizzare la tua esperienza.

Widget relativi alle tendenze

I seguenti widget mostrano i dati sulle tendenze relative alle esposizioni, alle minacce e alle risorse, in modo da poterli analizzare nel tempo.

Widget di panoramica delle tendenze



Questo widget mostra una panoramica delle tue esposizioni, minacce, risorse e scoperte nei seguenti periodi di tempo:

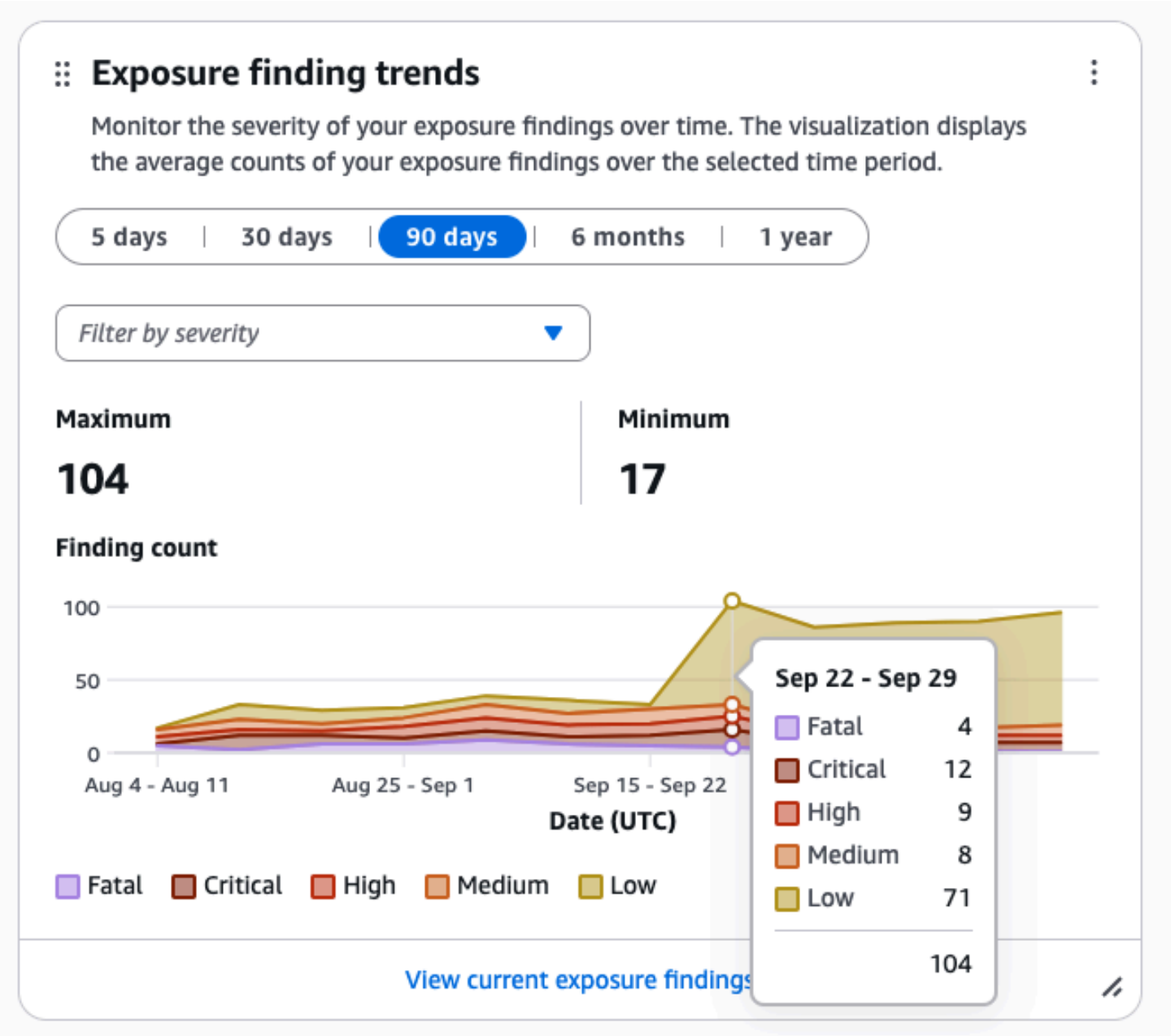
- Month-over-monthriflette il conteggio periodo per periodo degli ultimi due mesi.
- Week-over-weekriflette il conteggio periodo per periodo delle ultime due settimane.

- Day-over-dayriflette il conteggio periodo per periodo degli ultimi 2 giorni.

Il numero accanto alla percentuale riflette il conteggio medio per periodo fino ad oggi. Scegliendo questo numero si accede alla dashboard corrispondente nella console. Se accedi a un'altra dashboard che mostra i dati sulle tendenze, la dashboard mostra solo i dati sulle tendenze degli ultimi 90 giorni o nel periodo di tempo più adatto se il tuo account non contiene risultati o risorse più vecchi di 30 giorni.

> **Note**
>
> Per ricevere dati in questo widget, devi abilitare i seguenti servizi di sicurezza:
>
> - AWS Security Hub CSPM: per ricevere dati sulle esposizioni
> - Amazon Inspector — Per ricevere dati sulle esposizioni
> - GuardDuty— Per ricevere dati sulle minacce

Widget per la rilevazione dell'esposizione



Questo widget mostra la gravità dei risultati dell'esposizione nei seguenti periodi di tempo:

- 5 giorni
- 30 giorni
- 90 giorni
- 6 mesi
- 1 anno

La visualizzazione mostra il conteggio medio dei risultati nel periodo di tempo selezionato.

Filtri di gravità

Puoi aggiornare il grafico includendo o escludendo i seguenti filtri di gravità:

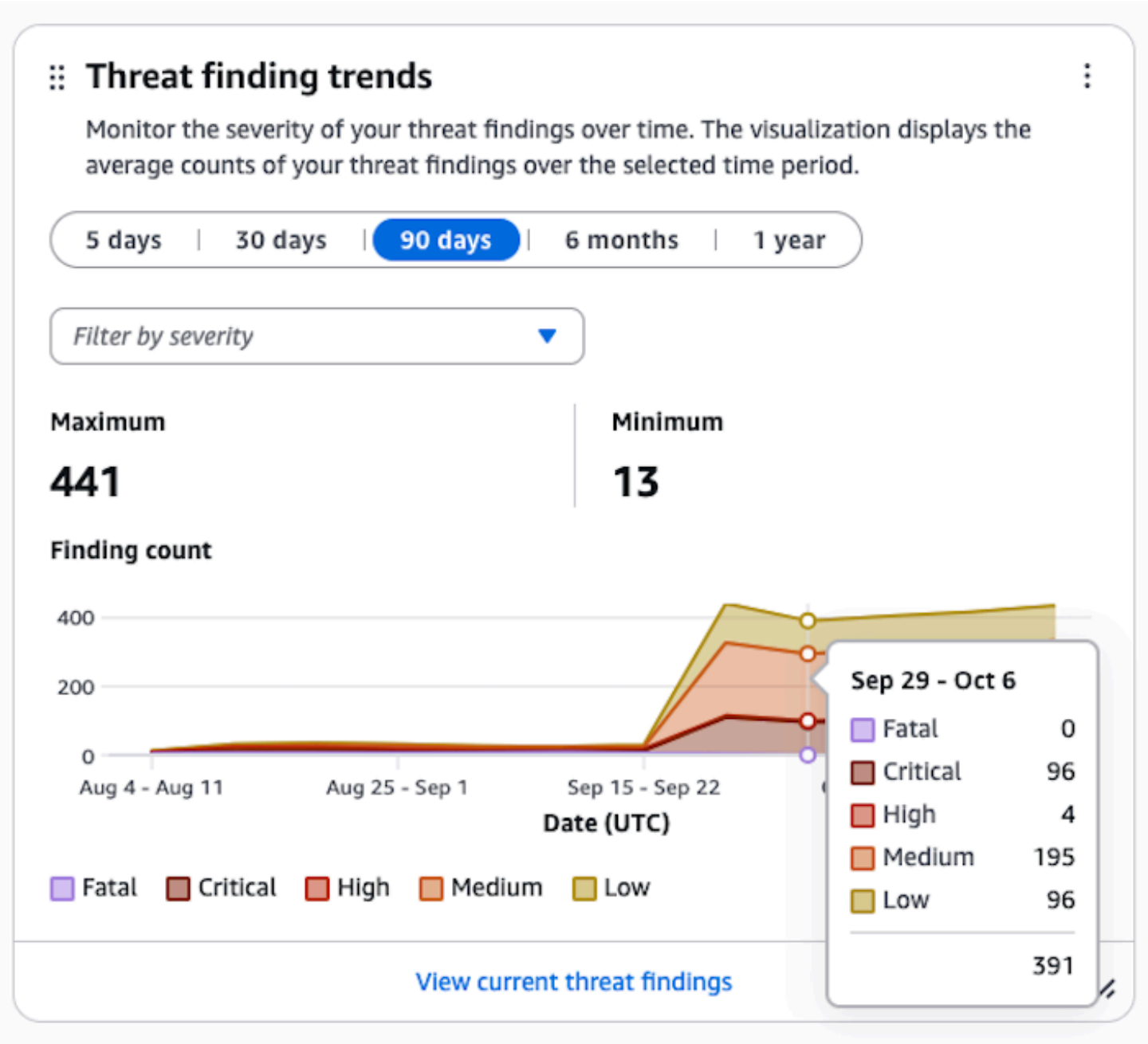
- Fatale
- Critico
- Elevate
- Medio
- Bassa
- Informativo
- Other (Altro)
- Sconosciuto

I filtri di gravità applicati vengono visualizzati nella parte inferiore della visualizzazione in diverse caselle. Puoi passare il mouse sulla visualizzazione per esaminare il conteggio medio dei risultati per momenti specifici. Puoi anche esaminare il numero medio di risultati che corrispondono a ciascun filtro di gravità applicato.

Puoi scegliere Visualizza tutti i risultati attuali sull'esposizione per essere indirizzati al pannello di controllo Esposizione. Per impostazione predefinita, la dashboard di Exposure mostra solo i dati sulle tendenze degli ultimi 90 giorni. Se il tuo account non contiene dati sull'esposizione più vecchi di 30 giorni, la dashboard mostra i dati sulle tendenze in base al periodo di tempo più adatto.

> **Note**
>
> Per ricevere dati in questo widget, devi abilitare Amazon Inspector e Security Hub CSPM.

Widget sulle tendenze di rilevamento delle minacce



Questo widget mostra la gravità delle minacce rilevate nei seguenti periodi di tempo:

- 5 giorni
- 30 giorni
- 90 giorni
- 6 mesi
- 1 anno

La visualizzazione mostra il conteggio medio dei risultati nel periodo di tempo selezionato.

Filtri di gravità

Puoi aggiornare il grafico includendo o escludendo i seguenti filtri di gravità:

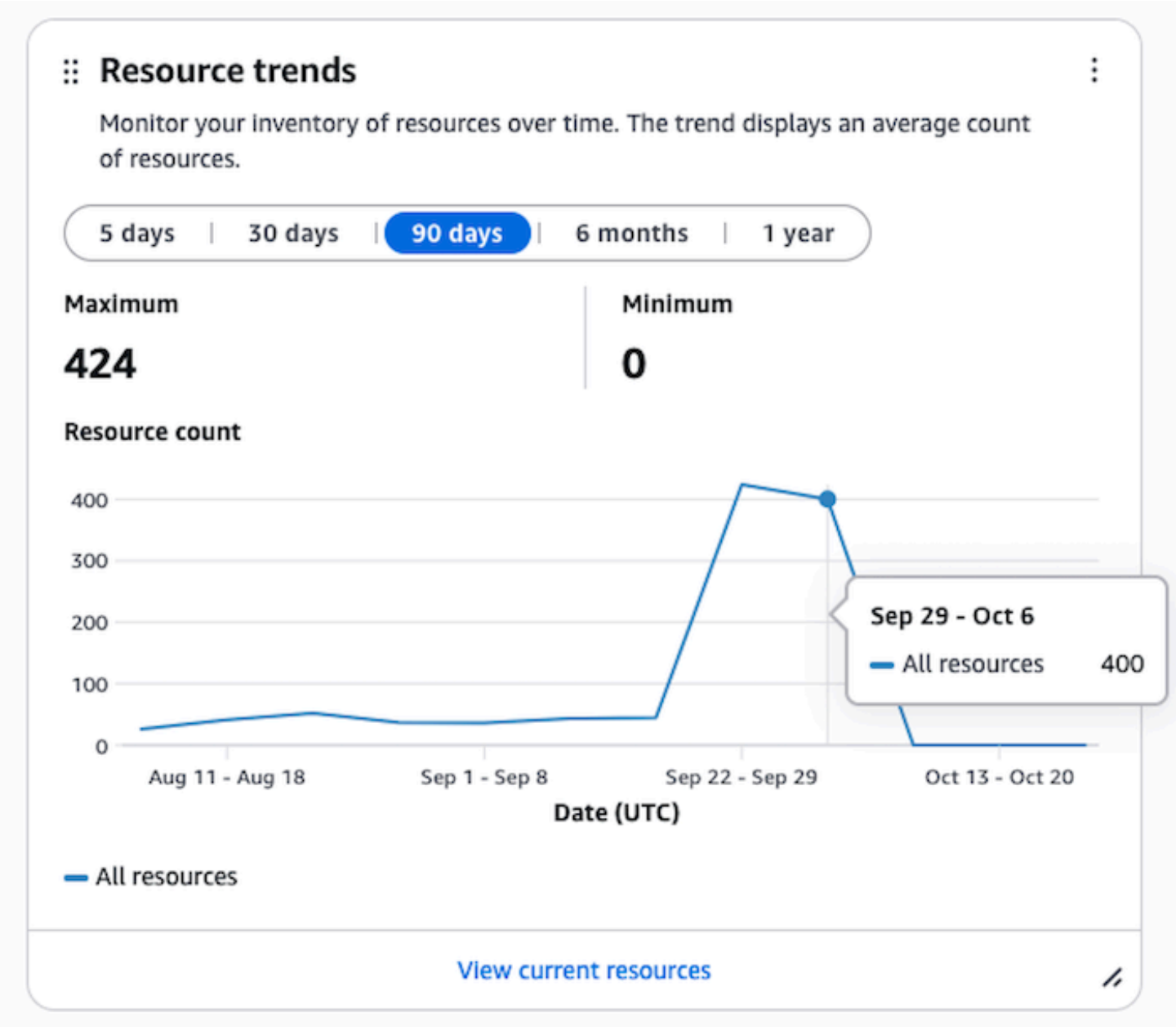
- Fatale
- Critico
- Elevate
- Medio
- Bassa
- Informativo
- Other (Altro)
- Sconosciuto

I filtri di gravità applicati vengono visualizzati nella parte inferiore della visualizzazione in diverse caselle. Puoi passare il mouse sulla visualizzazione per esaminare il conteggio medio dei risultati per momenti specifici. Puoi anche esaminare il numero medio di risultati che corrispondono a ciascun filtro di gravità applicato.

Puoi scegliere Visualizza tutti i risultati attuali delle minacce per essere indirizzato alla dashboard di Exposure. Per impostazione predefinita, la dashboard delle minacce mostra solo i dati sulle tendenze degli ultimi 90 giorni. Se il tuo account non contiene dati sulle minacce più vecchi di 30 giorni, la dashboard mostra i dati sulle tendenze in base al periodo di tempo più adatto.

> **Note**
>
> Per ricevere dati in questo widget, devi abilitare. GuardDuty

Widget sulle tendenze delle risorse



Questo widget mostra un inventario delle tue risorse nei seguenti periodi di tempo:

- 5 giorni
- 30 giorni
- 90 giorni
- 6 mesi
- 1 anno

La visualizzazione mostra il numero medio delle risorse nel periodo di tempo selezionato. Puoi passare il mouse sulla visualizzazione per esaminare il numero medio di risorse per momenti specifici.

Puoi scegliere Visualizza le risorse correnti per essere indirizzato alla dashboard Risorse. Per impostazione predefinita, la dashboard Risorse mostra solo i dati sulle tendenze degli ultimi 90 giorni. Se il tuo account non contiene risorse più vecchie di 30 giorni, la dashboard mostra i dati sulle tendenze in base al periodo di tempo più adatto.

Questo widget mostra un inventario delle tue risorse nei seguenti periodi di tempo:

- 5 giorni
- 30 giorni
- 90 giorni
- 6 mesi
- 1 anno

Conservazione dei dati per le tendenze

Security Hub conserva i dati sulle tendenze per un anno per tutti i dispositivi Account AWS in cui Security Hub è abilitato. Dopo che i dati sulle tendenze sono stati conservati per un anno, vengono eliminati da Security Hub.

I dati di tendenza per gli account amministratori delegati e autonomi vengono eliminati dopo la disattivazione di Security Hub o se gli account vengono chiusi.

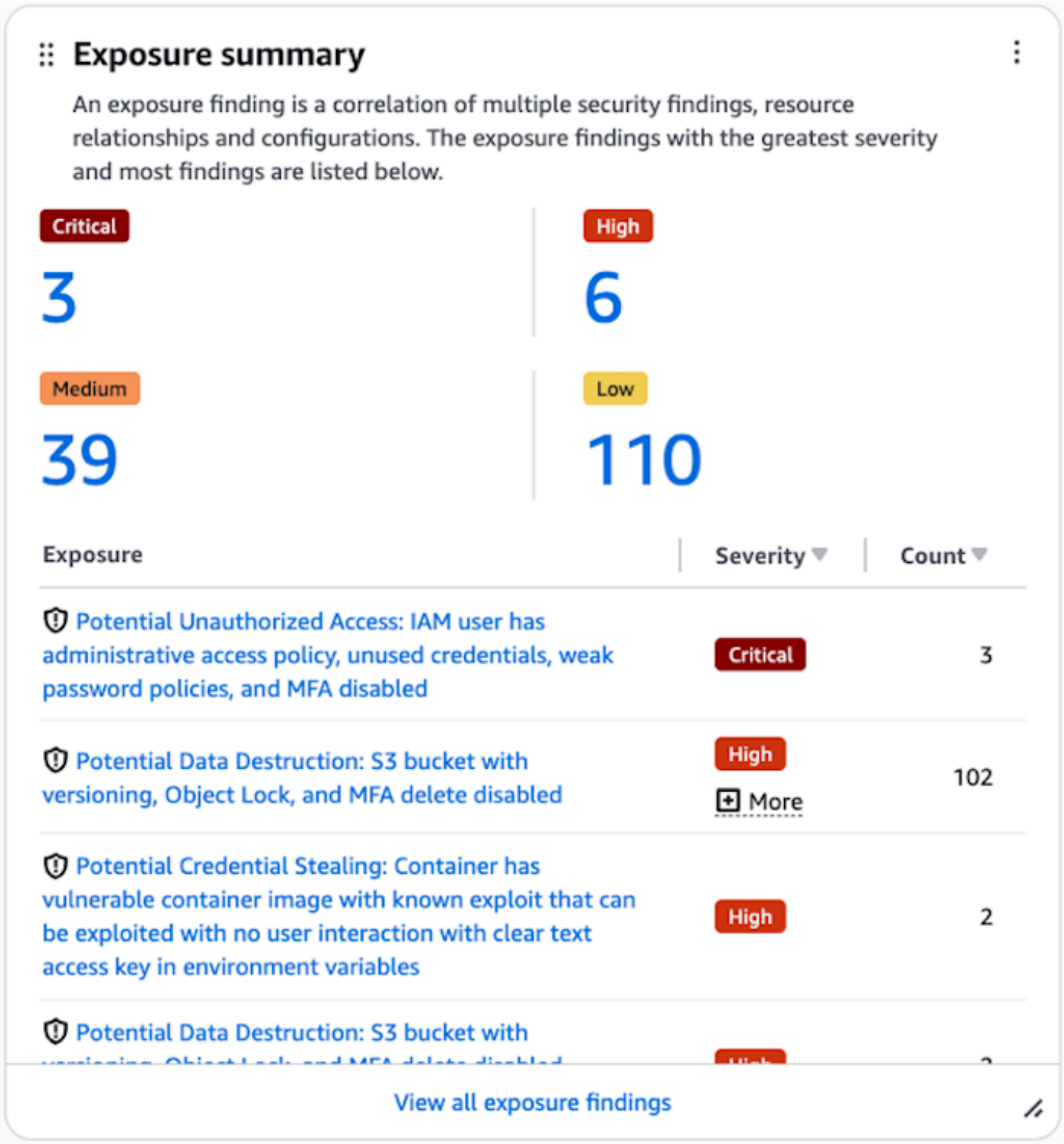
Scenari di conservazione dei dati di Trends per gli account membri con Security Hub abilitato:

- Se un account membro lascia la propria organizzazione, Security Hub conserva comunque i dati sulle tendenze, fino a quando l'account ha lasciato l'organizzazione, per un anno.
- Se Security Hub è disabilitato per un account membro, Security Hub conserva i dati sulle tendenze, fino a quando l'account è stato disabilitato, per un anno.
- Se un account membro viene chiuso, Security Hub dissocia i dati sulle tendenze dall'account chiuso (ad esempio, cancellando l'ID dell'account chiuso) e conserva il resto dei dati sulle tendenze per un anno.

Widget di riepilogo

I seguenti widget mostrano un riepilogo delle tue esposizioni, minacce e risorse.

widget di riepilogo dell'esposizione

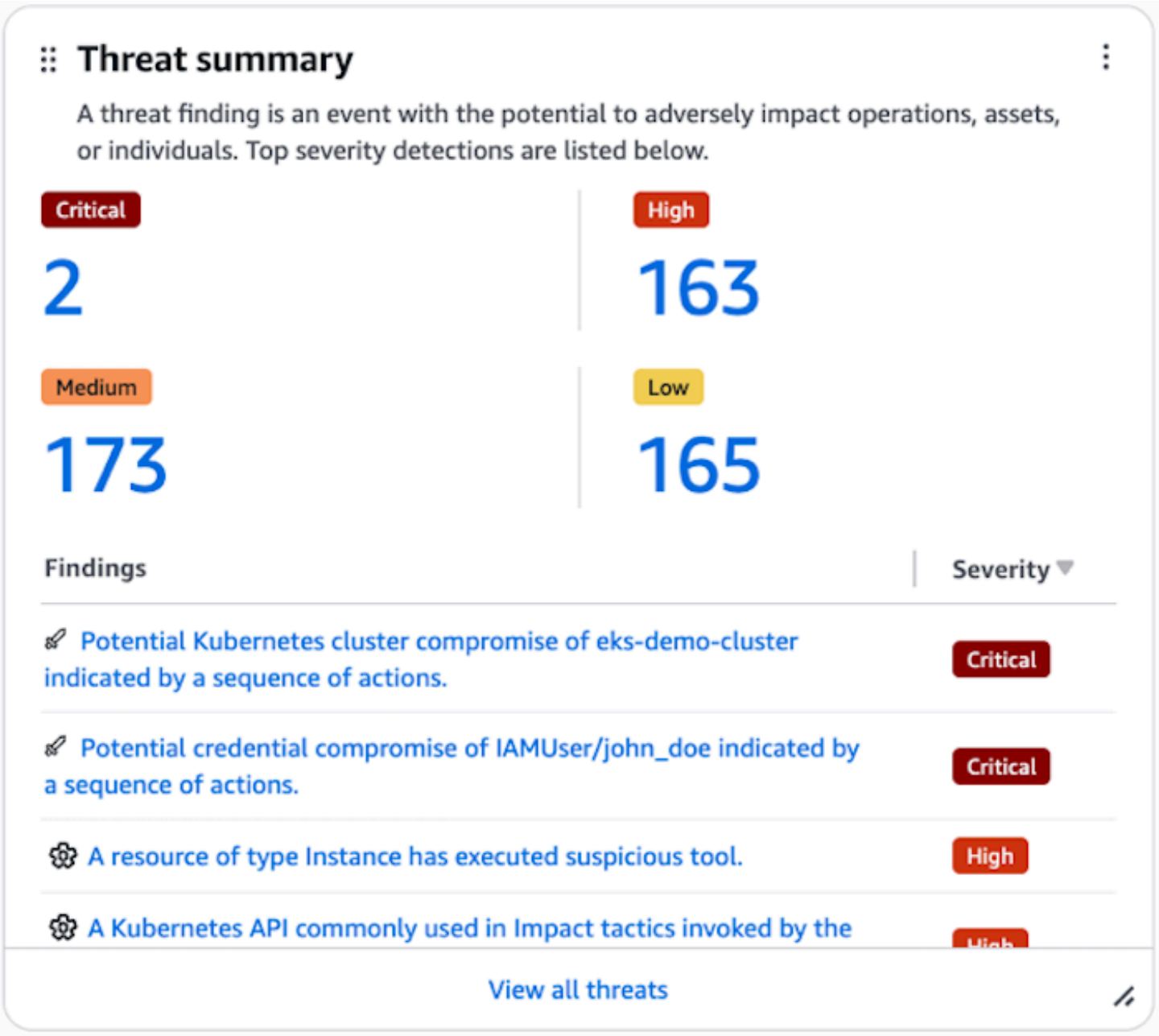


Questo widget mostra le tue esposizioni in base alla gravità. L'esposizione si basa su un'analisi dei risultati e delle caratteristiche di Security Hub e di altri servizi AWS di sicurezza, come Amazon

Inspector. L'elenco delle esposizioni in questo widget è limitato alle otto esposizioni con la massima severità. Le esposizioni con maggiore severità vengono visualizzate per prime nell'elenco. Se due o più esposizioni sono di uguale gravità, l'elenco raggruppa automaticamente tali esposizioni in base alle esposizioni più recenti. Scegliendo Visualizza tutte le esposizioni si accede al pannello di controllo Esposizioni.

> **Note**
>
> Per ricevere dati in questo widget, devi abilitare Amazon Inspector e Security Hub CSPM. https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-settingup.html

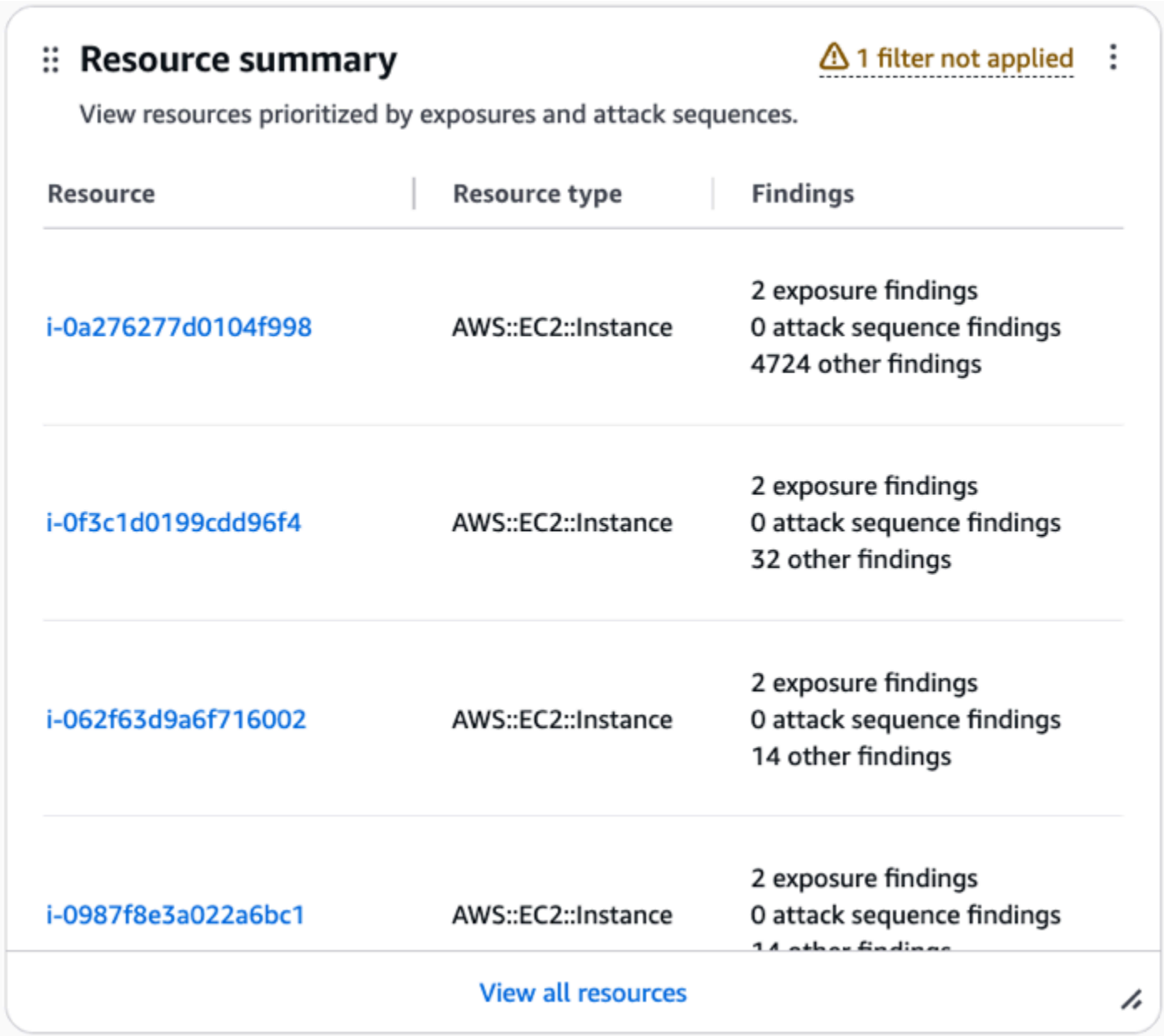
widget di riepilogo delle minacce



Questo widget mostra le minacce in base alla gravità. Una minaccia si riferisce ad attività dannose o sospette che possono compromettere la sicurezza dell'ambiente. L'elenco delle minacce in questo widget è limitato alle otto minacce con la massima gravità. Le minacce con maggiore severità vengono visualizzate per prime nell'elenco. Se due o più minacce hanno la stessa gravità, l'elenco raggruppa automaticamente tali minacce in base alle minacce più recenti. Scegliendo Visualizza tutte le minacce si accede alla dashboard delle minacce.

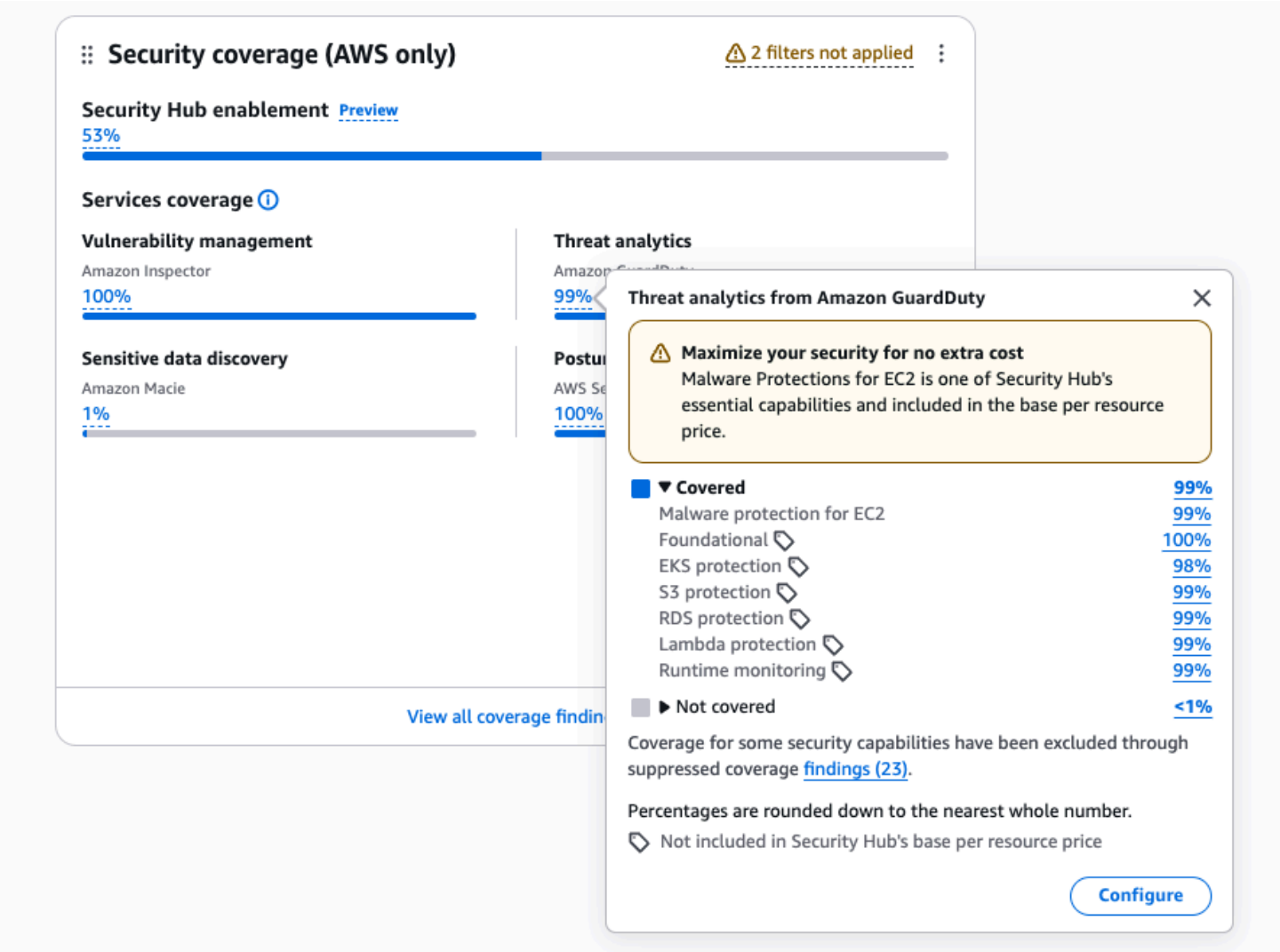
> **Note**
>
> Per ricevere dati in questo widget, devi abilitare. GuardDuty

widget di riepilogo delle risorse



Questo widget mostra le risorse per tipo e i risultati associati alle risorse. Alle risorse viene assegnata la priorità in base alle esposizioni e alle sequenze di attacco. Scegliendo Visualizza tutte le risorse si accede alla dashboard delle risorse.

Widget di copertura della sicurezza



Il widget mostra un riepilogo della copertura dell'account per le seguenti funzionalità di sicurezza:

- Gestione delle vulnerabilità da parte di Amazon Inspector
- Rilevamento delle minacce da parte di Amazon GuardDuty
- Rilevamento di dati sensibili da parte di Amazon Macie
- Gestione della postura tramite AWS Security Hub CSPM

Negli account di amministratore delegato, il widget mostra anche la copertura dell'account per l'abilitazione di Security Hub.

Ogni elemento di copertura mostra una percentuale che rappresenta l'attivazione di tale funzionalità nei tuoi account. La scelta di una percentuale consente di visualizzare i dettagli sulla copertura di

tale funzionalità. Se si sceglie la percentuale di attivazione di Security Hub, viene visualizzato un pannello laterale. Il pannello mostra quanti account sono abilitati in ogni regione dell'organizzazione.

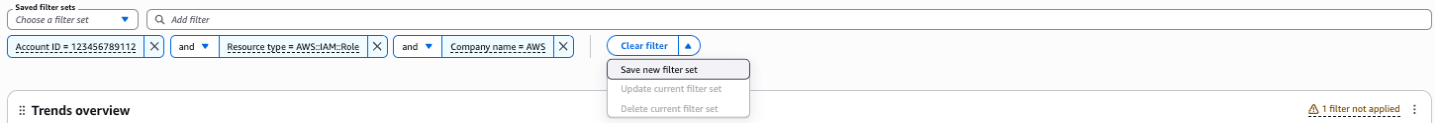
Nella sezione Copertura dei servizi, le percentuali rappresentano la percentuale di controlli di copertura superati per ciascuna funzionalità di sicurezza. Questi controlli riguardano gli account e le regioni in cui Security Hub è abilitato. Se si sceglie una percentuale di copertura, viene visualizzato un popover che suddivide ciascuna funzionalità come Coperta (controllo superato) o Non coperto (controllo fallito). Le percentuali vengono arrotondate per difetto al numero intero più vicino. Scegliendo una percentuale nel popover si apre la pagina dei risultati della copertura con i dettagli sui risultati che compongono quella percentuale. Scegli Configura per aprire il singolo servizio in cui puoi gestire la configurazione per quella funzionalità o per aprire la pagina delle configurazioni del Security Hub in cui puoi aggiornare le configurazioni per i servizi di sicurezza.

Se uno dei risultati della copertura in Security Hub viene eliminato, il widget mostra un messaggio che informa che la copertura è stata esclusa: la copertura per le funzionalità di sicurezza è stata esclusa attraverso i risultati della copertura soppressa.

Per ulteriori informazioni sulla visualizzazione e la soppressione dei risultati della copertura, vedi Risultati della copertura in Security Hub.

Filtri disponibili

Puoi applicare filtri ai widget di sicurezza utilizzando la barra Aggiungi filtro.



I filtri sono organizzati nelle seguenti categorie:

- Filtri condivisi: si applicano a tutti i widget di sicurezza
- Filtri di ricerca: si applica ai widget di sicurezza che visualizzano i dati di ricerca
- Filtri relativi alle risorse: si applica ai widget di sicurezza che visualizzano i dati delle risorse

Puoi creare un set di filtri collegando i filtri utilizzando gli operatori e/o e quindi scegliendo Salva nuovo set di filtri nel menu a discesa.

Filtri applicati al widget Exposure finding trends e Threat finding trends

Attualmente, i filtri supportati per questi widget includono quanto segue:

- ID account
- Ricerca del nome della classe
- Tipo di risultato
- Product name (Nome del prodotto)
- Region
- Stato

Filtri applicati al widget Tendenze delle risorse

Attualmente, i filtri supportati per questo widget includono quanto segue:

- ID account
- Region
- Categoria di risorse
- Tipo di risorsa

Filtri non applicati ai widget



Se un widget non supporta un filtro, il filtro non viene applicato al widget. In questo caso, il widget visualizza un messaggio di avviso che indica quanti filtri non sono stati applicati ed elenca i nomi dei filtri non supportati.

Visualizzazione dei dettagli sulle risorse in Security Hub

La pagina Risorse tiene traccia delle risorse comuni dell'account e dell'organizzazione. Puoi accedere alla pagina Risorse nella console di Security Hub scegliendo Risorse nel riquadro di navigazione. Il vantaggio della pagina Risorse è che consente di monitorare il livello di sicurezza, organizzare le risorse e rivedere i dettagli sulle risorse. Quando scegli un tipo di risorsa, puoi esaminare tutte le risorse associate al tipo di risorsa. È possibile esaminare qualsiasi risultato associato a una risorsa. I tipi di risorse disponibili nella pagina Risorse includono tutte le risorse dei tuoi account coperte dai servizi AWS di sicurezza che contribuiscono ai risultati di Security Hub.

> **Note**
>
> L'amministratore delegato può visualizzare tutte le risorse associate agli account dei membri. Se hai configurato una home page Regione AWS, puoi visualizzare tutte le risorse presenti nella home page Regione AWS da Linked Regioni AWS.

Se scegli una risorsa, puoi esaminarne i dettagli. Questi dettagli includono il nome, l'ID, l'ARN, il tipo e la categoria della risorsa. È possibile esaminare l'ID dell'account associato alla risorsa, la data di creazione della risorsa (timestamp) e il luogo in cui è stata creata la risorsa ().Regione AWSÈ inoltre possibile esaminare ulteriori dettagli di configurazione sulla risorsa. Questi dettagli sono disponibili in uno snippet JSON che puoi copiare.

Se passi dalla scheda Panoramica alla scheda Risultati, puoi esaminare tutti i risultati associati alla risorsa. La scheda Risultati mostra il nome di ogni risultato, il tipo di ogni risultato e la gravità di ogni risultato. Puoi raggruppare i risultati in diversi campi e cercarli utilizzando i filtri. Se scegli un risultato, puoi esaminarne una panoramica, che include informazioni sulla conformità e su come risolvere i problemi associati al risultato. La scheda Caratteristiche mostra ogni caratteristica identificata sulla risorsa. È possibile visualizzare le caratteristiche che contribuiscono a determinare l'esposizione della risorsa. Puoi anche vedere le caratteristiche contestuali, che sono altri elementi di sicurezza identificati per la risorsa ma che non hanno contribuito direttamente ai risultati dell'esposizione. Se torni alla risorsa, puoi scegliere Apri risorsa per esaminare la risorsa nella console in base al tipo di risorsa. Ad esempio, se la risorsa è una risorsa IAM, puoi aprirla nella console IAM.

La pagina delle risorse offre diversi modi per organizzare e cercare le risorse. È possibile raggruppare le risorse per tipo. Ad esempio, è possibile raggruppare le risorse per ID account, tipo di ricerca Regione AWS, categoria di risorsa, nome della risorsa e tipo di risorsa. I filtri rapidi consentono di esaminare le risorse per categoria, account e tipi di ricerca.

Security Hub e Open Cybersecurity Schema Framework (OCSF)

Security Hub utilizza l'Open Cybersecurity Schema Framework (OCSF) come formato standard per tutti i risultati di sicurezza. Questo argomento descrive OCSF e come Security Hub lo implementa.

Panoramica dell'OCSF

I risultati di Security Hub sono formattati utilizzando OCSF (Open Cybersecurity Schema Framework). OCSF è un progetto open source che offre un framework estensibile per lo sviluppo di schemi,

insieme a uno schema di sicurezza di base indipendente dal fornitore. I fornitori e altri produttori di dati possono adottare ed estendere lo schema per i loro domini specifici. I produttori di dati possono mappare schemi diversi per aiutare i team addetti alla sicurezza a semplificare l'inserimento e la normalizzazione dei dati, in modo che i data scientist e gli analisti possano lavorare con un linguaggio comune per il rilevamento e l'indagine delle minacce. L'obiettivo è fornire uno standard aperto, adottato in qualsiasi ambiente, applicazione o soluzione, integrando al contempo gli standard e i processi di sicurezza esistenti.

Il framework è costituito da tipi di dati, un dizionario degli attributi e una tassonomia. Sebbene non si limiti alla sicurezza informatica o agli eventi, l'attenzione iniziale è rivolta agli schemi degli eventi di sicurezza informatica. L'OCSF è indipendente dal formato di archiviazione, dai metodi di raccolta dei dati e dai processi ETL.

Security Hub attualmente supporta i risultati della versione 1.6 dello schema OCSF.

Risorse correlate

Per ulteriori informazioni su OCSF e sulla sua implementazione, consulta le seguenti risorse:

- Documentazione OCSF pubblica
- Documentazione sull'utilizzo delle estensioni OCSF
- Riferimento allo schema di base OCSF
- Registro delle estensioni OCSF

AWS estensione per OCSF

Gli schemi OCSF possono essere estesi aggiungendo nuovi attributi, oggetti, categorie, profili e classi di eventi. Uno schema è l'aggregazione delle entità e delle estensioni dello schema principale.

Le estensioni a OCSF consentono a un particolare fornitore o cliente di ampliare uno schema esistente aggiungendo attributi per fornire una personalizzazione specifica del dominio, migliorare l'interoperabilità dei dati e aggiungere un contesto più dettagliato per l'analisi della sicurezza.

L' AWS Extension for Open Cybersecurity Schema Framework (OCSF) fornisce definizioni di attributi per le risorse cloud all'interno degli eventi OCSF. Questa estensione aggiunge un `cloud_resources` profilo che estende l'oggetto OCSF con attributi di risorse specifici `resource_details` del cloud. Con questi attributi, i team di sicurezza possono analizzare le configurazioni delle risorse, le potenziali vulnerabilità e i metadati di rilevamento delle minacce.

Oggetto resource_details esteso

L' AWS estensione estende l'`resource_details`oggetto con gli attributi menzionati nell'elenco dei riferimenti agli attributi riportato di seguito. Questi attributi garantiscono la corretta identificazione e classificazione delle risorse cloud tra diversi provider all'interno di framework di eventi standardizzati.

AWS Estensione per il riferimento agli attributi OCSF

Le sezioni Attributi di base e Oggetti specifici per le risorse forniscono esempi di ciascuno degli attributi che fanno parte dell'estensione AWS OCSF a resource_details.

Ciascuna delle definizioni degli attributi contiene uno stato OCSF che ne delinea la relazione corrente con lo schema OCSF pubblico:

- Esistente: questo attributo era già presente nello standard OCSF resource_details e ora fa parte dell'estensione. AWS
- Nuovo: l'attributo non fa parte dell'OCSF ed è stato introdotto come parte dell'estensione. AWS Non esiste nello schema OCSF principale.
- Aggiunto a resource_details: l'attributo è definito in OCSF ma non fa parte di resource_details.

Attributi di base

Si tratta di attributi fondamentali utilizzati per l'identificazione, la posizione e i metadati di base delle risorse. Sono costituiti da tipi di dati semplici come stringhe, timestamp e array.

Partizione cloud

La partizione cloud in cui esiste la risorsa.

Requisito

Consigliato

Tipo

Stringa

Stato OCSF

Esistente

Esempio

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

ID dell'account del proprietario

Un identificatore di account a 12 cifre a cui appartiene la risorsa.

Requisito

Consigliato

Tipo

Stringa

Stato OCSF

Esistente

Esempio

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

Tipo di risorsa

Il tipo di AWS CloudFormation risorsa che identifica il servizio e la risorsa specifici.

Requisito

Richiesto

Tipo

Stringa

Formato

Deve seguire la convenzione di denominazione dei tipi di AWS CloudFormation risorsa: `AWS::<Service>::<ResourceType>`

Stato OCSF

Esistente

Esempio

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

Identificatore di risorsa

L'identificatore univoco della risorsa cloud (ad esempio, i-1234567890abcdef0).

Requisito

Consigliato

Tipo

Stringa

Formato

Deve essere un identificatore di risorsa valido. Lunghezza minima pari a 1. Lunghezza massima di 768.

Stato OCSF

Esistente

Esempio

```
{
  "resources": [
    {
      "uid": "i-1234567890abcdef0"
    }
  ]
}
```

Identificatore di risorsa alternativo

L'identificatore univoco per la risorsa cloud, in genere Amazon Resource Name (ARN).

Requisito

Consigliato

Tipo

Stringa

Formato

Dovrebbe essere un ARN valido AWS . I modelli più comuni includono:

- `"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"`

Nota: alcuni servizi come S3 utilizzano varianti come arn:aws:s3: ::bucket-name (senza regione o ID account).

Stato OCSF

Esistente

Esempi

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

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

Nome risorsa

Il nome univoco della risorsa cloud.

Requisito

Consigliato

Tipo

Stringa

Formato

User-created nomi i cui valori dipenderanno dall'ambiente.

stato OCSF

Esistente

Esempio

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

```
  ]
}
```

Regione cloud

La AWS regione in cui si trova la risorsa.

Requisito

Consigliato

Tipo

Stringa

Formato

Identificatore valido della regione cloud (ad esempio, us-east-1, eu-west-1, ap-southeast-2)

Stato OCSF

Esistente

Esempio

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

Ora di creazione della risorsa

L'ora in cui la risorsa è stata creata.

Requisito

Consigliato

Tipo

Time stamp

Formato

Timestamp Unix in millisecondi dall'epoca (1 gennaio 1970, 00:00:00 UTC)

Stato OCSF

Esistente

Esempio

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

Tag

Key-value coppie per i metadati e l'organizzazione delle risorse.

Requisito

Consigliato

Tipo

Matrice di oggetti chiave:value

Formato

Un oggetto generico che consente di definire una coppia chiave:valore.

Stato OCSF

Esistente

Esempio

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

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

IP address (Indirizzo IP)

L'indirizzo IP associato all'istanza in formato IPv4 o IPv6.

Requisito

Facoltativo

Tipo

Stringa

Formato

Indirizzo IPv4 o IPv6 valido

Stato OCSF

Esistente

Esempio

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

```
}
```

Indcirizzi IP

Una serie di indirizzi IP (IPv4 o IPv6) associati al dispositivo. Questi possono includere indirizzi IP pubblici e privati.

Requisito

Facoltativo

Tipo

Matrice di indirizzi IP

Stato OCSF

Novità

Esempio

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

UID VPC

L'ID VPC in cui si trova la risorsa.

Requisito

Facoltativo

Tipo

Stringa

Formato

Identificatore VPC (ad esempio, vpc-12345678900)

Stato OCSF

Aggiunto a `resource_details`

Esempio

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

Esempio di oggetto risorsa con attributi di base

```
{
  "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"
    }
  ]
}
```

Oggetti specifici per le risorse

Si tratta di oggetti annidati complessi che forniscono informazioni dettagliate per tipi di risorse e servizi specifici. Ogni oggetto contiene più campi e sottooggetti con configurazione e metadati specifici del servizio.

Dispositivo

Attributi avanzati delle istanze cloud per le risorse di calcolo, tra cui dettagli di crittografia, informazioni sull'immagine, profilo dell'istanza e ora di avvio.

Requisito

Facoltativo

Tipo

Oggetto

Stato OCSF

Aggiunto a. `resource_details` Vedi la definizione dell'oggetto OCSF Device.

AWS L'estensione aggiunge i seguenti attributi a questo oggetto:

- `encryption_details`- I dettagli di crittografia della risorsa
- `image`- Informazioni sull'immagine
- `instance_profile`- Il profilo dell'istanza IAM da associare all'istanza
- `launch_time`- L'ora in cui l'istanza è stata avviata
- `uid_alt`- Amazon Resource Name (ARN) della risorsa

Esempio


```
{
  "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"
  }
}
```

Interfaccia di rete

Dettagli e configurazione dell'interfaccia di rete, inclusi allegati e gruppi di sicurezza.

Requisito

Facoltativo

Tipo

Oggetto

Stato OCSF

Aggiunto a. `resource_details` Vedere la definizione dell'oggetto OCSF Network Interface.

AWS L'estensione aggiunge i seguenti attributi a questo oggetto:

- `attachments`- Informazioni sugli allegati dell'interfaccia di rete
- `security_groups`- Serie di identificatori univoci dei gruppi di sicurezza
- `uid_alt`- Amazon Resource Name (ARN) della risorsa

Esempio

```
{
  "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"
      }
    ]
  }
}
```

Dispositivo di archiviazione

Dettagli del dispositivo di archiviazione, inclusi allegati, crittografia e informazioni sulle istantanee.

Requisito

Facoltativo

Tipo

Oggetto

Stato OCSF

Novità

L'oggetto del dispositivo di archiviazione include i seguenti attributi:

- `name`- Il nome del dispositivo di archiviazione
- `uid`- L'identificatore univoco del dispositivo di archiviazione
- `attachments`- Gli allegati del dispositivo di archiviazione
- `encryption_details`- La chiave di crittografia del dispositivo di archiviazione
- `is_encrypted`- Se il dispositivo di archiviazione è crittografato (obbligatorio)
- `snapshot_id`- L'identificatore dell'istantanea del dispositivo di archiviazione
- `uid_alt`- Amazon Resource Name (ARN) della risorsa

Esempio

```
{
  "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"
  }
}
```

Database

Attributi dell'istanza del database, tra cui tipo di motore, endpoint e informazioni sull'utente.

Requisito

Facoltativo

Tipo

Oggetto

Stato OCSF

Aggiunto a. `resource_details` Vedere la definizione dell'oggetto del database OCSF.

AWS L'estensione aggiunge i seguenti attributi a questo oggetto:

- `cluster_uid`- L'identificatore del cluster del database
- `db_endpoint`- L'endpoint del database
- `encryption_details`- I dettagli di crittografia del database
- `engine`- Il nome del motore del database (ad esempio, mysql)
- `is_encrypted`- Se il database è crittografato
- `is_iam_authentication`- Se l'autenticazione IAM è abilitata
- `is_public`- Se il database è accessibile al pubblico
- `port`- Il numero di porta del database
- `security_groups`- Matrice di gruppi di sicurezza VPC associati all'istanza del database
- `snapshot_details`- I dettagli dell'istantanea del database
- `status`- Lo stato del database (ad esempio, disponibile)
- `subnet_group`- Un gruppo di sottoreti di database è una raccolta di sottoreti in un VPC
- `uid_alt`- Amazon Resource Name (ARN) della risorsa
- `user`- L'utente del database
- `version`- La versione del database

Esempio

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

Cluster di database

Attributi dell'istanza del database, tra cui tipo di motore, endpoint e informazioni sull'utente.

Requisito

Facoltativo

Tipo

Oggetto

Stato OCSF

Novità

L'oggetto del database include i seguenti attributi:

- `uid`- L'identificatore univoco del cluster di database
- `uid_alt`- Amazon Resource Name (ARN) della risorsa
- `name`- Il nome del cluster di database
- `status`- Lo stato del cluster di database
- `engine`- Il motore associato al cluster
- `version`- La versione del cluster di database
- `cluster_members`- Elenco delle istanze di database che fanno parte del cluster
- `security_groups`- Matrice di gruppi di sicurezza associati al cluster
- `is_encrypted`- Se il cluster di database è crittografato
- `is_iam_authentication`- Se l'autenticazione IAM è abilitata
- `encryption_details`- I dettagli di crittografia del cluster di database
- `subnet_group`- Il gruppo di sottorete associato al cluster
- `port`- Il numero di porta del cluster di database
- `zones`- Elenco delle zone di disponibilità
- `db_endpoint`- L'endpoint del cluster di database
- `snapshot_details`- Dettagli dello snapshot del database

Esempio

```
{
```

```
  "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
    }
  }
}
```

Funzione cloud

Attributi delle funzioni cloud per funzioni serverless, tra cui configurazione di gestori, livelli e runtime.

Requisito

Facoltativo

Tipo

Oggetto

Stato OCSF

Novità

L'oggetto cloud function include i seguenti attributi:

- `name`- Il nome della funzione cloud
- `uid`- L'identificatore univoco della funzione cloud
- `uid_alt`- Amazon Resource Name (ARN) della risorsa
- `encryption_details`- I dettagli della crittografia della funzione cloud
- `handler`- Il metodo nel codice della funzione che elabora gli eventi
- `layers`- L'elenco dei livelli funzionali cloud che contengono codice o dati supplementari
- `runtime`- L'ambiente specifico della lingua delle funzioni cloud
- `security_groups`- Serie di gruppi di sicurezza associati alla funzione cloud
- `subnet_info_list`- Dettagli sulle sottoreti associate alla funzione cloud
- `user`- Dettagli sull'entità IAM che concede a cloud_function il permesso di accedere ai servizi
- `version`- La versione della funzione cloud
- `vpc_uid`- L'identificatore univoco del VPC se la funzione cloud è in un VPC

Esempio

```
{
  "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"
  }
}
```

Databucket

Bucket S3 o attributi di archiviazione dei dati.

Requisito

Facoltativo

Tipo

Oggetto

Stato OCSF

Aggiunto a. `resource_details` Vedi la definizione dell'oggetto OCSF Databucket.

Nota: questo oggetto viene aggiunto a resource_details dall'estensione. AWS L'oggetto principale di OCSF Databucket viene utilizzato senza attributi aggiuntivi.

Esempio

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

Immagine

Informazioni sulle immagini per le risorse di calcolo, inclusi dettagli sulla piattaforma e sull'utilizzo.

Requisito

Facoltativo

Tipo

Oggetto

Stato OCSF

Aggiunto a. `resource_details` Vedi la definizione dell'oggetto OCSF Image.

AWS L'estensione aggiunge i seguenti attributi a questo oggetto:

- `platform`- La piattaforma del sistema operativo dell'immagine
- `in_use_count`- Numero di risorse che utilizzano questa immagine

Esempio

```
{
  "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
  }
}
```

Informazioni sulla sottorete

Dettagli sulla sottorete in cui si trova la risorsa.

Requisito

Facoltativo

Tipo

Oggetto

Stato OCSF

Novità

L'oggetto info sulla sottorete include i seguenti attributi:

- `uid`- L'identificatore univoco della sottorete
- `uid_alt`- Amazon Resource Name (ARN) della risorsa
- `name`- Il nome della sottorete
- `zone`- La zona di disponibilità
- `ip_count`- Il numero di indirizzi IP nella sottorete
- `cidr_block`- Il blocco CIDR della sottorete
- `is_default`- Se si tratta della sottorete predefinita
- `is_public`- Se la sottorete è accessibile al pubblico
- `state`- Lo stato della sottorete
- `vpc_uid`- L'ID VPC in cui si trova la sottorete

Esempio

```
{
  "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"
  }
}
```

Utente

Attributi utente IAM, inclusi i profili e le policy delle istanze.

Requisito

Facoltativo

Tipo

Oggetto

Stato OCSF

Aggiunto a. `resource_details` Vedi la definizione dell'oggetto utente OCSF.

L'oggetto utente include i seguenti attributi:

- `instance_profiles`- Elenco dei profili di istanza collegati a un'istanza cloud
- `policies`- Politiche che assegnano autorizzazioni per utenti, gruppi, ruoli e risorse

Esempio

```
{
  "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"
      }
    ]
  }
}
```

Risultati della copertura in Security Hub

I risultati della copertura per Security Hub forniscono visibilità su quali funzionalità di AWS sicurezza sono abilitate e dove potrebbero esserci lacune nella copertura in un account autonomo o tra gli account membri di un'organizzazione. I risultati della copertura attualmente supportano la segnalazione dei servizi e delle funzionalità abilitati per Amazon GuardDuty, Amazon Inspector, Amazon Macie e AWS Security Hub CSPM. Questi esiti vengono visualizzati nel widget Security Coverage sulla dashboard di Security Hub, con la possibilità di accedere a visualizzazioni più dettagliate per funzionalità di sicurezza specifiche.

Limitazioni

- Per gli account membri, le informazioni sulla copertura vengono aggregate tra tutti gli account collegati Regioni AWS, ma solo per quell'account membro.
- Le informazioni sulla copertura non vengono visualizzate per gli account non collegati a Security Hub.

Risultati della copertura per AWS Security Hub CSPM

I risultati della copertura CSPM di Security Hub valutano se in un account è abilitato uno standard di sicurezza qualificato per la gestione della postura. L'abilitazione di qualsiasi standard CSPM di Security Hub è idonea, ad eccezione degli standard Resource Tagging e Resource Tagging. AWS Control Tower

Possono essere necessarie fino a 24 ore per rilevare gli standard abilitati per impostazione predefinita quando si abilita Security Hub CSPM.

Risultati della copertura per Amazon GuardDuty

GuardDuty i risultati della copertura valutano se GuardDuty è abilitata e quali GuardDuty funzionalità sono abilitate in un Account AWS:

- GuardDuty Protezione da malware per Amazon EC2: analizza le istanze di Amazon EC2 alla ricerca di potenziali malware.
- GuardDuty Amazon EKS Protection: monitora i log di audit di Kubernetes alla ricerca di minacce nei cluster Amazon EKS.
- GuardDuty Lambda Protection: analizza le chiamate alle funzioni Lambda alla ricerca di potenziali minacce.
- GuardDuty Amazon S3 Protection: analizza gli eventi relativi ai dati alla ricerca di potenziali minacce ai bucket Amazon S3.
- GuardDuty Amazon RDS Protection: monitora le minacce ai database Amazon RDS.
- GuardDuty Monitoraggio del runtime: fornisce il monitoraggio in tempo reale del comportamento di runtime nelle istanze Amazon EC2.
- GuardDuty Copertura fondamentale: GuardDuty funzionalità di base che vengono attivate automaticamente quando sono abilitate. GuardDuty

> **Note**
>
> Per quanto riguarda GuardDuty Foundational Coverage, i risultati della copertura che indicano che la funzionalità è disattivata indicano che non GuardDuty è abilitata nell'account per il rilevamento della copertura.

Possono essere necessarie fino a 24 ore prima che gli aggiornamenti della GuardDuty copertura vengano applicati a tutti gli account dei membri di un'organizzazione.

Risultati della copertura per Amazon Inspector

I risultati della copertura di Amazon Inspector valutano se Amazon Inspector è abilitato e quali funzionalità sono abilitate in un account:

- Scansione EC2 di Inspector: analizza le istanze Amazon EC2 alla ricerca di vulnerabilità.
- Inspector ECR Scanning: analizza le immagini dei container Amazon ECR alla ricerca di vulnerabilità.
- Inspector Lambda Standard Scanning: analizza le funzioni Lambda alla ricerca di vulnerabilità.
- Inspector Lambda Code Scanning: analizza le funzioni del codice Lambda alla ricerca di vulnerabilità del codice.

Risultati della copertura per Amazon Macie

I risultati della copertura di Macie valutano se Macie è abilitato in: Account AWS

- Copertura automatizzata per il rilevamento dei dati sensibili di Macie: valuta continuamente il tuo patrimonio di dati Amazon S3 alla ricerca di dati sensibili.

Gli aggiornamenti del rilevamento automatico dei dati sensibili di Macie possono richiedere fino a 24 ore affinché i risultati della copertura si riflettano in tutti gli account dei membri di un'organizzazione.

Soppressione dei risultati della copertura

Per impostazione predefinita, i risultati della copertura di sicurezza valutano quali funzionalità CSPM di Amazon GuardDuty, Amazon Inspector, Amazon Macie e AWS Security Hub sono abilitate per un account e una regione. Se alcune funzionalità di sicurezza non sono applicabili per te o rappresentano un rischio accettato, puoi utilizzare la funzione di soppressione per eliminare i risultati della copertura in modo simile a tutti gli altri risultati. Quando un dato di copertura viene eliminato, non viene incluso nei calcoli della copertura all'interno del widget relativo alla copertura di sicurezza. Il widget visualizza il seguente messaggio: La copertura per le funzionalità di sicurezza è stata esclusa tramite i risultati della copertura soppressi. Il messaggio include un conteggio dei risultati soppressi.

Per eliminare una rilevazione della copertura in Security Hub

1. Quando visualizzi il widget sulla copertura di sicurezza, scegli il link relativo alla percentuale di copertura.
2. Dal popup sulla copertura, scegli Visualizza i risultati della copertura. Ogni risultato con lo stato Nuovo delinea un divario di copertura osservato.
3. Selezionate la casella di controllo accanto a ogni risultato da eliminare.

4. Nella parte superiore della pagina, scegli Stato dell'aggiornamento, quindi scegli Soppresso.
5. Nella finestra di dialogo Imposta lo stato su Soppresso, potete inserire facoltativamente una nota che specifichi il motivo della modifica dello stato. Quindi scegliete Imposta lo stato.

Inventario AI nel Security Hub

L'inventario AI in AWS Security Hub offre una visione unificata delle risorse di intelligenza artificiale (AI) e machine learning (ML) in tutto l' AWS ambiente. Usa l'inventario dell'intelligenza artificiale per identificare carichi di lavoro AI non autorizzati, capire dove viene eseguita l'IA e come è stata scoperta e dare priorità alle risorse che richiedono una revisione più approfondita della sicurezza. Security Hub organizza le risorse AI in due tipi di discovery:

- Gestito: risorse di intelligenza artificiale AWS fornite come servizio gestito. Security Hub rileva queste risorse dagli elementi AWS Config di configurazione. I tipi di risorse gestite includono un sottoinsieme supportato di Amazon Bedrock, Amazon Bedrock AgentCore e Amazon. SageMaker
- Self-hosted— Risorse di intelligenza artificiale che non vengono fornite come servizio gestito. Gli esempi includono modelli open source, agenti e server di inferenza eseguiti sul tuo computer. Security Hub rileva che queste risorse generano segnali sulle istanze Amazon Elastic Compute Cloud (Amazon EC2) e sulle immagini di Amazon Elastic Container Registry (Amazon ECR). I segnali includono i risultati della distinta base del software Amazon Inspector (SBOM) e l'attività di Amazon DNS. GuardDuty

Gli account amministratore possono visualizzare le risorse AI di tutti gli account abilitati della loro organizzazione. Gli account dei membri possono visualizzare solo le risorse di intelligenza artificiale all'interno del proprio account.

Prerequisiti per la scoperta dell'IA ospitata autonomamente

L'individuazione di risorse AI gestite non richiede alcuna configurazione aggiuntiva oltre all'abilitazione di Security Hub. Per scoprire le risorse di intelligenza artificiale ospitate autonomamente, devi anche abilitare quelle Servizi AWS che forniscono i segnali che contribuiscono:

- Amazon Inspector: abilita Amazon Inspector (con Security Hub essentials) per generare SBOM. Security Hub utilizza questi SBOM per rilevare modelli, endpoint di inferenza e agenti ospitati autonomamente. Per le istanze Amazon EC2, abilita la scansione basata su agenti con modalità di scansione avanzata, scansione senza agente o scansione ibrida. Agent-based la scansione senza modalità di scansione avanzata non produce l'inventario software completo richiesto dal

rilevamento delle risorse AI. Per le immagini Amazon ECR, Amazon Inspector fornisce SBOM tramite la scansione delle immagini dei container.

- Amazon GuardDuty: abilita GuardDuty in modo che Security Hub possa utilizzare l'attività DNS per rilevare gli endpoint AI esterni richiamati dalle tue istanze Amazon EC2.

Tipi di risorse AI supportati

In base alla disponibilità generale, Security Hub supporta i seguenti tipi di risorse AI ospitate autonomamente. Security Hub utilizza un sistema di rilevamento basato sulla fiducia per risorse AI ospitate autonomamente. Ogni rilevamento è ancorato a un segnale primario, ad esempio un componente SBOM. Security Hub mette quindi in correlazione segnali aggiuntivi per stabilire la fiducia prima che una risorsa compaia nel tuo inventario. Security Hub mostra solo le risorse che soddisfano la soglia di confidenza, il che aiuta a ridurre al minimo i falsi positivi. Ogni risorsa utilizza un `ResourceType` `SelfHosted::AI::` prefisso.

- Modelli (`SelfHosted::AI::Model`) - Modelli Hugging Face e Ollama. Security Hub rileva i modelli solo nelle directory predefinite della cache dei modelli (come le cache Hugging Face e Ollama) e nei percorsi personalizzati configurati per la scansione di Amazon Inspector.
- Inference endpoints (`SelfHosted::AI::InferenceEndpoint`) — Software di model-serving supportato, come VLLM, Ollama TorchServe, Triton, Text Generation Inference (TGI), sGLang, llama.cpp, LocalAI, BentoML, Xinference, Ray Serve e GPT4all.
- Agenti `SelfHosted::AI::Agent` () OpenClaw — agenti.
- Endpoint esterni (`SelfHosted::AI::ExternalEndpoint`): domini di servizi AI esterni richiamati dalle tue istanze Amazon EC2. Security Hub mantiene un elenco consentito di domini di servizi AI noti, come OpenAI, Anthropic, Cohere, Mistral e altri importanti provider di intelligenza artificiale, e rileva quando le tue istanze inviano loro richieste DNS. Gli endpoint esterni vengono rilevati solo dall'attività GuardDuty DNS su Amazon EC2.

Le risorse AI gestite sono un sottoinsieme supportato dei tipi di elementi di SageMaker configurazione Amazon Bedrock, Amazon Bedrock AgentCore e Amazon, ciascuno con la `AI/ML` categoria di risorse.

Ricerca di risorse AI dalla pagina Risorse

La pagina Risorse elenca tutte le risorse del tuo ambiente. Per le risorse di intelligenza artificiale, puoi utilizzare le seguenti funzionalità per identificare i carichi di lavoro AI e gli host che li eseguono:

- AI/ML Le risorse gestite visualizzano un'icona AI accanto alla risorsa. Scegli l'icona per visualizzare una descrizione.
- Le risorse host che eseguono risorse di intelligenza artificiale ospitate autonomamente, come le istanze Amazon EC2, mostrano un badge di conteggio AI ospitato autonomamente. Gli host che non dispongono di risorse di intelligenza artificiale ospitate autonomamente non visualizzano alcun badge.
- Utilizza l'interruttore rapido del filtro per mostrare solo gli host che contengono risorse AI ospitate autonomamente.
- Per approfondire un host, scegli l'host per aprirne il pannello dei dettagli, scegli la scheda Risorse AI, quindi scegli Visualizza tutto per vedere le risorse AI ospitate autonomamente rilevate su quell'host.

Utilizzando la pagina dell'inventario AI

La pagina dell'inventario AI si concentra sulle risorse AI della tua organizzazione. Ogni risorsa in questa pagina appartiene alla categoria di `AI/ML` risorse. Questa pagina mostra le risorse AWS AI gestite e le risorse AI ospitate autonomamente nel tuo ambiente. Le sezioni seguenti descrivono i componenti principali della pagina.

Barra di riassunto

La barra di riepilogo mostra il numero totale di risorse di intelligenza artificiale e una suddivisione per tipo di scoperta, ospitate autonomamente o gestite. Mostra anche una suddivisione per sottocategoria, ad esempio modello o agente. Scegliete il valore di una statistica per visualizzare i dettagli di supporto nella tabella.

Raggruppamento, filtraggio e ricerca

Per impostazione predefinita, la tabella di inventario AI raggruppa le risorse per tipo di risorsa. È possibile modificare il raggruppamento o rimuoverlo per una visualizzazione semplice di tutte le risorse. I campi di raggruppamento disponibili includono ID canonico, tipo di risorsa host, tipo di scoperta, ID account e tipo di risorsa.

L'ID canonico identifica cos'è una risorsa, indipendentemente da dove viene eseguita. Ad esempio, due istanze Amazon EC2 che eseguono lo stesso modello Hugging Face condividono lo stesso ID canonico, in modo da poter trovare tutte le implementazioni di un modello specifico nell'organizzazione.

> **Note**
>
> I raggruppamenti di ID canonici e tipi di risorse host si applicano solo alle risorse ospitate autonomamente. Quando si raggruppano in base a questi campi, le risorse AI gestite non vengono visualizzate nei risultati perché non hanno questi attributi. Utilizza i raggruppamenti dei tipi di rilevamento o dei tipi di risorse per visualizzare insieme le risorse gestite e quelle ospitate autonomamente.

I filtri rapidi consentono di filtrare per sottocategoria di risorse o tipo di scoperta. I filtri di proprietà supportano campi aggiuntivi, tra cui il tipo di risorsa host e l'ID canonico per le risorse ospitate autonomamente.

Dettagli sulle risorse e segnali di contributo

Scegliete una riga di risorse per aprire il pannello dei dettagli. Per le risorse gestite, il pannello visualizza la configurazione delle risorse come JSON. Per le risorse ospitate autonomamente, il pannello mostra i segnali che contribuiscono utilizzati da Security Hub per rilevare la risorsa. Questi segnali includono la fonte di rilevamento e i dettagli dei singoli segnali, come i componenti SBOM e il software di inferenza di supporto per un modello o il dominio DNS per un endpoint esterno.

Trasferimento alla risorsa host

Per una risorsa AI ospitata autonomamente, il pannello dei dettagli mostra la risorsa host in cui Security Hub ha rilevato la risorsa. Per visualizzare tutte le risorse AI ospitate autonomamente sullo stesso host, filtra la tabella in base alla risorsa host. Con questa visualizzazione, puoi eseguire il drill-up da una singola risorsa ospitata autonomamente al relativo host ed esaminare le risorse AI adiacenti su quell'host.

Considerazioni

L'inventario AI presenta le seguenti limitazioni in base alla disponibilità generale:

- Self-hosted Le risorse di intelligenza artificiale non hanno risultati in questa versione. Security Hub mostra il numero di risultati solo per le risorse AI gestite.
- Self-hosted Il rilevamento AI è supportato solo sulle istanze Amazon EC2 e sulle immagini Amazon ECR. AWS Lambda le funzioni e altri tipi di elaborazione non sono supportati.
- Security Hub non attribuisce le immagini Amazon ECR a un host principale in questa versione, quindi i conteggi AI degli host non le includono.

- Security Hub rileva gli endpoint esterni dall'attività GuardDuty DNS solo su Amazon EC2. In questa versione, Security Hub non attribuisce le chiamate da AWS Fargate, AWS Lambda Amazon, SageMaker Amazon EKS o altre elaborazioni gestite dal servizio.

Accesso all'inventario AI con l'API

Puoi recuperare i dati dell'inventario AI in modo programmatico con la GetResourcesV2 e le operazioni. GetResourcesStatisticsV2

Per AI/ML le risorse, la `GetResourcesV2` risposta include i campi e. `ResourceSubCategory` `DiscoveryType` Il `DiscoveryType` campo indica se una risorsa è `Managed` o`SelfHosted`. Per le risorse AI ospitate autonomamente e le relative risorse host, la risposta include anche `ResourceInfo` una `AIDetails` struttura.

Self-hosted Le risorse di intelligenza artificiale utilizzano un `ResourceType` con il `SelfHosted::AI::` prefisso. I tipi supportati includono i seguenti:

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

La `AIDetails` struttura collega una risorsa AI ospitata autonomamente al relativo host con i `HostResourceType` campi `HostResourceGuid` and. Il `CanonicalId` campo identifica cos'è una risorsa, indipendentemente da dove viene distribuita, in modo da poter aggregare risorse identiche su più host. L'ID canonico utilizza un formato: `type/identifier`

- Per i modelli ML: `model/<purl>` (ad esempio,) `model/pkg:huggingface/meta-llama/llama-3-8b`
- Per endpoint e agenti di inferenza: un formato `type/asset-identifier-name`
- Per gli endpoint esterni: il dominio normalizzato (ad esempio,) `api.*.openai.com`

Su una risorsa host, ad esempio un'istanza Amazon EC2, `SelfHostedAI*ResourceCount` i campi e il `SelfHostedTotalAIResourceCount` campo contengono i conteggi delle risorse AI ospitate autonomamente rilevate sull'host.

Note

Quando si utilizza `GetResourcesV2` e si filtra per`ResourceSubCategory`, è necessario includere anche un `ResourceCategory` filtro. Imposta il confronto su `EQUALS` e il valore su`AI/ML`. Questo requisito si applica anche quando si esegue il `ResourceSubCategory` raggruppamento per o `ResourceInfo.AIDetails.CanonicalId` in base a`GetResourcesStatisticsV2`. `ResourceInfo.AIDetails.HostResourceType` Altrimenti, l'operazione restituisce un`ValidationException`.
L'esempio seguente mostra una combinazione di filtri valida:

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

Risorse in Security Hub

Security Hub assegna un livello di criticità a ciascuna risorsa dell'ambiente. La criticità indica l'importanza di una risorsa per l'azienda e aiuta a dare priorità alle attività di sicurezza. La criticità è una delle`Very High`,,`High`, `Medium` o. `Low` `Unknown`

In che modo Security Hub individua la criticità

Per impostazione predefinita, Security Hub deduce la criticità dai segnali sulla risorsa:

- Nome della risorsa: Security Hub corrisponde ai modelli nel nome della risorsa. Ad esempio, una risorsa con `pci` o `prod` nel nome viene considerata più importante di una risorsa denominata`sandbox`.
- Tag: Security Hub corrisponde ai modelli nei tag delle risorse. Ad esempio, una risorsa etichettata con `environment=production` viene considerata più importante di una con tag`environment=dev`.

Sovrascrivere la criticità con una regola di automazione

È possibile ignorare la criticità dedotta creando una regola di automazione che imposta esplicitamente la criticità sulle risorse che soddisfano i criteri della regola. Una regola di automazione ha sempre la precedenza sulla criticità dedotta. Per ulteriori informazioni, consulta Azioni e criteri relativi alle regole delle risorse.

In che modo la criticità influisce sull'esposizione, individuandone la gravità

Security Hub utilizza la criticità delle risorse come input per calcolare l'impatto e la gravità di un rilevamento dell'esposizione. Le risorse con una criticità pari a non influiscono sulla `Unknown` gravità del rilevamento dell'esposizione. Per ulteriori informazioni, consulta Impatto.

Esiti relativi alle esposizioni in Security Hub

Un risultato di esposizione in Security Hub rappresenta la correlazione di più segnali di sicurezza che identificano i potenziali rischi per la sicurezza nell' AWS ambiente in uso. I risultati sull'esposizione ti aiutano a comprendere e dare priorità ai rischi per la sicurezza. Analizzano automaticamente combinazioni di vulnerabilità, configurazioni, minacce e relazioni tra le risorse. Un risultato

sull'esposizione include tratti e segnali. Un segnale può includere uno o più tipi di caratteristiche di esposizione. Security Hub genera un risultato di esposizione quando i segnali provenienti da Security Hub CSPM, Amazon Inspector GuardDuty, Macie o AWS altri servizi indicano la presenza di un'esposizione. Una risorsa può essere la risorsa principale in, al massimo, un rilevamento dell'esposizione. Se una risorsa non presenta caratteristiche di esposizione o presenta caratteristiche insufficienti, Security Hub non genera un risultato di esposizione per quella risorsa.

Come funzionano i risultati dell'esposizione

Security Hub genera risultati sull'esposizione mediante:

Analisi dei segnali provenienti da più servizi AWS di sicurezza

Security Hub raccoglie e analizza continuamente i segnali di sicurezza provenienti da più servizi AWS di sicurezza. Acquisisce i risultati GuardDuty per il rilevamento delle minacce, Amazon Inspector per la valutazione delle vulnerabilità, Security Hub CSPM per i controlli di configurazione e Macie per l'esposizione dei dati sensibili. Questi segnali vengono elaborati tramite motori di correlazione avanzati per identificare potenziali rischi per la sicurezza.

Valutazione delle configurazioni e delle relazioni tra le risorse

Il sistema esegue una valutazione dettagliata delle configurazioni delle risorse rispetto alle migliori pratiche di sicurezza. Esamina le impostazioni specifiche del servizio, i requisiti di conformità e i controlli di sicurezza. Questa analisi aiuta a identificare configurazioni errate che potrebbero portare a vulnerabilità di sicurezza se combinate con altri fattori.

Valutazione della raggiungibilità della rete

Una componente cruciale dei risultati dell'esposizione è la valutazione della raggiungibilità della rete. Il sistema valuta sia l'esposizione a Internet che i percorsi di accesso alla rete interna. Analizza le configurazioni dei gruppi di sicurezza e le impostazioni ACL di rete per determinare i potenziali vettori di attacco. Questa analisi aiuta a identificare le risorse che potrebbero essere inavvertitamente esposte ad accessi non autorizzati.

Correlazione dei problemi di sicurezza correlati

Il motore di correlazione mappa le relazioni tra le AWS risorse, analizzando il modo in cui interagiscono e identificando le potenziali implicazioni per la sicurezza. Esamina le autorizzazioni, i ruoli e i modelli di accesso alle risorse di IAM per comprendere il contesto di sicurezza più ampio. Questo processo aiuta a identificare i rischi per la sicurezza che potrebbero esistere a causa della combinazione di configurazioni individuali apparentemente innocenti.

Componenti di un rilevamento dell'esposizione

Ciascun risultato dell'esposizione include:

Titolo e descrizione del potenziale rischio per la sicurezza

Ogni risultato sull'esposizione include un titolo chiaro e descrittivo che comunica immediatamente la natura del rischio per la sicurezza. La descrizione fornisce informazioni dettagliate sul potenziale impatto sulla sicurezza, sulle risorse interessate e sul contesto più ampio dell'esposizione. Queste informazioni aiutano i team addetti alla sicurezza a comprendere e valutare rapidamente il rischio.

Classificazione della gravità (critica, alta, media, bassa)

- La gravità critica indica che è necessaria un'attenzione immediata a causa dell'elevata probabilità di exploit e del significativo impatto potenziale. Questi risultati rappresentano in genere vulnerabilità facilmente individuabili e sfruttabili.
- Un'elevata severità suggerisce che è necessaria un'attenzione prioritaria, con una probabilità di exploit da moderata a elevata e un impatto potenziale sostanziale. Questi risultati potrebbero essere relativamente facili da sfruttare, ma potrebbero richiedere condizioni specifiche.
- Una severità media indica che è necessaria un'attenzione programmata, con una minore probabilità di exploit e un impatto potenziale moderato. Questi risultati richiedono in genere metodi di sfruttamento più complessi.
- Un livello di severità basso indica che è necessaria un'attenzione di routine, con un potenziale di exploit limitato e un impatto minore. Questi risultati sono in genere difficili da sfruttare e presentano un rischio minimo.

Tratti che hanno contribuito all'esposizione

I tratti che contribuiscono rappresentano i fattori principali che hanno portato alla scoperta dell'esposizione. I tratti che contribuiscono includono quanto segue:

- Vulnerabilità di sicurezza dirette
- Problemi di configurazione
- Condizioni di esposizione della rete
- Impostazioni delle autorizzazioni delle risorse
- Criticità delle risorse (l'importanza di una risorsa per l'azienda)

Ogni caratteristica fornisce dettagli specifici su come contribuisce al rischio complessivo per la sicurezza.

Visualizzazione del percorso di attacco potenziale e del raggio di esplosione

La visualizzazione del percorso di attacco potenziale e del raggio di esplosione fornisce un diagramma interattivo che mostra come i potenziali aggressori potrebbero sfruttare l'esposizione identificata. Associa le relazioni tra le risorse, i percorsi di rete e i percorsi di escalation dei privilegi alle risorse a valle che sono potenzialmente accessibili a un utente malintenzionato se l'esposizione viene sfruttata.

Linee guida dettagliate sulla riparazione

Ogni rilevazione dell'esposizione include una guida dettagliata sulla riparazione con misure specifiche e attuabili per affrontare i rischi identificati. Queste linee guida includono raccomandazioni sulle migliori pratiche, passaggi di correzione della configurazione e azioni prioritarie. La guida è personalizzata in base allo scenario di esposizione specifico e considera i AWS servizi coinvolti.

Dettagli sulla configurazione delle risorse

Configurazione della risorsa al momento della creazione del risultato e configurazione corrente della risorsa nella dashboard dell'inventario delle risorse del Security Hub.

Tratti contestuali che forniscono un contesto di sicurezza aggiuntivo

I tratti contestuali sono indicatori di sicurezza aggiuntivi che sono stati identificati da Security Hub ma non sono stati utilizzati per creare un risultato di esposizione.

Le informazioni di accesso non utilizzate provenienti da IAM Access Analyzer possono apparire come caratteristiche contestuali nei risultati dell'esposizione. Quando un ruolo IAM collegato a una risorsa dispone di autorizzazioni non utilizzate, Security Hub include queste informazioni come caratteristica contestuale nella visualizzazione dei dettagli dell'esposizione. Ad esempio, se un'istanza Amazon EC2 presenta una vulnerabilità software e il ruolo IAM associato ha 47 autorizzazioni non utilizzate su 5 servizi, il risultato dell'esposizione mostra le autorizzazioni non utilizzate come contesto supplementare. Questo ti aiuta a comprendere il potenziale raggio di esplosione: una risorsa vulnerabile con un ruolo IAM troppo privilegiato presenta un rischio maggiore rispetto a una con autorizzazioni con privilegi minimi, perché una risorsa compromessa potrebbe utilizzare quelle autorizzazioni non utilizzate per aumentare l'accesso.

I seguenti tipi di risorse possono mostrare caratteristiche contestuali di accesso non utilizzate nei risultati di esposizione:

- Istanze Amazon Elastic Compute Cloud

- AWS Lambda funzioni
- Servizi Amazon Elastic Container Service
- Cluster Amazon Elastic Kubernetes Service
- Utenti IAM (direttamente)

Classificazione della gravità

I risultati dell'esposizione sono classificati in base a:

- Facilità di scoperta
- Facilità di sfruttamento
- Probabilità di sfruttamento
- Sensibilizzazione del pubblico
- Impatto potenziale
- Criticità delle risorse primarie

Per ulteriori informazioni, vedere Classificazione della gravità dei risultati di esposizione.

Vantaggi dei risultati dell'esposizione

- Analisi manuale ridotta grazie alla correlazione automatizzata: i risultati dell'esposizione riducono significativamente il tempo e l'impegno necessari per l'analisi della sicurezza attraverso la correlazione automatizzata e l'assegnazione intelligente delle priorità dei rischi. Security Hub monitora continuamente l' AWS ambiente, identificando e correlando automaticamente i rischi per la sicurezza che potrebbero essere ignorati attraverso la revisione manuale.
- Visualizzazione prioritaria dei rischi per la sicurezza: Security Hub utilizza sofisticati algoritmi di valutazione del rischio per dare priorità alle esposizioni in base a gravità, impatto, criticità delle risorse e probabilità di exploit. Questo aiuta i team addetti alla sicurezza a concentrare i propri sforzi innanzitutto sui rischi più significativi, migliorando l'efficienza delle operazioni di sicurezza.

Fonti di rilevazione dell'esposizione

I risultati sull'esposizione comprendono dati provenienti da:

- GuardDuty L'integrazione con Amazon offre funzionalità di rilevamento continuo delle minacce all'interno dei risultati di esposizione. Monitora attività dannose, potenziali compromissioni degli account e anomalie comportamentali. Il sistema incorpora queste scoperte sulle minacce in un'analisi più ampia dell'esposizione, aiutando a identificare quando le minacce si combinano con altri problemi di sicurezza per creare rischi significativi.
- Amazon Inspector fornisce dati cruciali sulla valutazione delle vulnerabilità ai risultati dell'esposizione. Fornisce informazioni dettagliate sulla raggiungibilità della rete, sulle vulnerabilità del software e sulle violazioni delle best practice di sicurezza. Questa integrazione aiuta a capire come le vulnerabilità potrebbero essere sfruttate attraverso percorsi di attacco identificati.
- AWS Security Hub CSPM garantisce che la conformità della configurazione e gli standard di sicurezza siano presi in considerazione nell'analisi dell'esposizione. Valuta le risorse rispetto ai controlli di sicurezza e alle migliori pratiche consolidati, fornendo una base per comprendere i rischi basati sulla configurazione.
- Amazon Macie migliora i risultati dell'esposizione con funzionalità di individuazione e classificazione dei dati sensibili. Identifica dove sono presenti dati sensibili all'interno dell' AWS ambiente e valuta i potenziali rischi per la privacy, aiutando a comprendere il potenziale impatto delle esposizioni identificate.

Best practice

- Esamina regolarmente i risultati sull'esposizione: una gestione efficace dell'esposizione richiede processi di revisione strutturati. Le organizzazioni devono implementare revisioni giornaliere delle esposizioni critiche, valutazioni settimanali dello stato di esposizione complessivo, analisi mensili delle tendenze e valutazioni trimestrali del livello di sicurezza. Questo approccio a più livelli garantisce un'attenzione adeguata sia ai rischi immediati che alle tendenze di sicurezza a lungo termine.
- Dai priorità alle esposizioni critiche e ad alta gravità: una gestione efficace dell'esposizione dipende da un'efficace prioritizzazione dei rischi. Le organizzazioni dovrebbero concentrarsi innanzitutto sulle esposizioni critiche, considerando al contempo la criticità delle risorse e l'impatto aziendale. Questo approccio basato sul rischio aiuta a garantire che gli sforzi di sicurezza siano in linea con le priorità aziendali e a massimizzare la riduzione del rischio.
- Implementazione delle fasi correttive consigliate: la correzione dell'esposizione deve seguire un approccio sistematico. Le organizzazioni devono implementare con attenzione le misure correttive consigliate, conservare una documentazione dettagliata delle modifiche, condurre test approfonditi delle modifiche e convalidare l'efficacia delle correzioni implementate. Questo

approccio metodico aiuta a garantire un'efficace mitigazione del rischio evitando al contempo conseguenze indesiderate.

- Configura le regole di risposta automatizzate: massimizzare il valore dei risultati dell'esposizione richiede un'automazione efficace. Le organizzazioni devono implementare regole di risposta automatizzate, configurare notifiche appropriate, stabilire flussi di lavoro efficienti e mantenere audit trail completi. Questa automazione aiuta a garantire una risposta coerente e tempestiva alle esposizioni identificate, riducendo al contempo lo sforzo manuale.

Tipi di risorse supportati per i risultati dell'esposizione in Security Hub

AWS Security Hub genera risultati sull'esposizione per i seguenti tipi di AWS risorse:

- `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`

Se disponi di un connettore Azure, Security Hub genera anche risultati sull'esposizione per i seguenti tipi di risorse di Azure:

- `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 genera un rilevamento dell'esposizione per risorsa principale. Se una risorsa non presenta caratteristiche di esposizione o presenta caratteristiche insufficienti, Security Hub non genera un risultato di esposizione per quella risorsa.

Tipi di caratteristiche supportati in Security Hub

AWS Security Hub genera un risultato di esposizione quando i risultati del controllo CSPM di AWS Security Hub e i risultati generati da altri supporti Servizi AWS, come Amazon Inspector, contengono caratteristiche di esposizione per una risorsa. La tabella seguente fornisce informazioni sui tipi di caratteristiche supportati.

Tipo di tratto	Description	Origine	Risorse interessate
Presupponibilità	Indica una risorsa con autorizzazioni fornite AWS Identity and Access Management	Configurazione delle risorse da AWS Config	AWS risorse con AWS Identity and Access Management ruoli associati
Impatto	Indica il raggio di esplosione potenziale se la risorsa viene compromessa, in base alle autorizza zioni effettive dei AWS Identity and Access Management responsab ili associati, inclusa la capacità di creare e modificare risorse, la criticità delle risorse a valle e la criticità della risorsa primaria.	• Analisi efficace delle autorizza zioni dei principali associati. AWS Identity and Access Management • Criticità delle risorse accessibili da un determina to preside. AWS Identity and Access Management La criticità può	AWS risorse con identità associate AWS Identity and Access Management

Tipo di tratto	Description	Origine	Risorse interessate
		essere stabilita dalle regole di automazione oppure verrà dedotta in base al nome e ai tag della risorsa.	
Configurazione errata	Indica una risorsa configurata in modo errato	AWS Risultati del controllo CSPM di Security Hub, rilevazioni delle GuardDuty minacce Amazon e informazioni sulla conferma delle risorse in. AWS Config	Tutti i tipi di risorse
Raggiungibilità	Indica i percorsi di rete aperti verso una risorsa	AWS Risultati del controllo CSPM di Security Hub, rilevazioni delle GuardDuty minacce di Amazon e risultati della raggiungi bilità della rete Amazon Inspector.	Istanze Amazon EC2, cluster Amazon EKS, funzioni Lambda e bucket Amazon S3

Tipo di tratto	Description	Origine	Risorse interessate
Dati sensibili	Indica che una risorsa contiene dati sensibili	Rilevamenti di dati sensibili di Macie	Bucket Amazon S3
Vulnerabilità	Indica che una risorsa presenta un punto debole che potrebbe essere sfruttato da una fonte di minaccia.	Rilevamenti di vulnerabilità del pacchetto Amazon Inspector e risultati di malware Amazon Amazon EC2 GuardDuty .	Istanze Amazon EC2, servizi Amazon ECS, cluster Amazon EKS e funzioni Lambda
Criticità	Indica l'importanza di una risorsa per l'azienda	Assegnato tramite regole di automazione. Se la criticità non è impostata da una regola di automazione, Security Hub la deduce dal nome e dai tag della risorsa. Per ulteriori informazioni, consulta Risorse in Security Hub.	Tutti i tipi di risorse

Ogni caratteristica può essere associata a più titoli che forniscono dettagli sull'esposizione che influisce sulla risorsa. Ad esempio, potresti vedere il titolo Exploit Available per il tratto Vulnerabilità nei dettagli di un risultato di esposizione EC2.

Impatto e autorizzazioni efficaci

Il tratto Impact descrive il raggio di esplosione potenziale di un'esposizione, vale a dire le risorse a valle che un aggressore potrebbe raggiungere e compromettere se la risorsa principale oggetto del rilevamento dell'esposizione viene compromessa. Per determinare l'impatto, Security Hub analizza le autorizzazioni effettive dei principali AWS Identity and Access Management (IAM) associati alla risorsa, nonché la criticità delle risorse.

Le autorizzazioni effettive sono le autorizzazioni effettivamente di cui dispone un principale dopo che Security Hub ha valutato le sue politiche basate sull'identità insieme alle politiche basate sulle risorse delle risorse a cui può accedere e tutte le politiche di controllo dei servizi (SCP) e le politiche di controllo delle risorse (RCP) dell' AWS Organizations applicabili all'account. Poiché le autorizzazioni efficaci tengono conto di ciò che viene concesso a un responsabile, delle risorse target consentite e dei limiti a livello di organizzazione che vincolano l'account, riflettono in modo più accurato le azioni che un responsabile può eseguire rispetto alle sole politiche basate sull'identità.

Utilizzando autorizzazioni efficaci, Security Hub traccia i percorsi di escalation dei privilegi dalla risorsa principale alle altre risorse dell'ambiente. Ogni percorso è una catena di risorse collegate da autorizzazioni che consentono a un utente malintenzionato di passare da una risorsa all'altra. Quando Security Hub identifica un percorso concreto verso una risorsa esistente, evidenzia quel percorso come parte del tratto Impact. Impact tiene conto anche delle autorizzazioni Servizi AWS che vanno oltre a questi percorsi, come la possibilità di invocare per creare o modificare altre risorse e la criticità della risorsa principale. Puoi esaminare questi percorsi nel grafico del percorso di attacco potenziale e ridurre il raggio di esplosione rimuovendo le autorizzazioni non necessarie. Per ulteriori informazioni, consulta Visualizzazione delle esposizioni in Security Hub con il grafico del percorso del potenziale attacco.

Generazione di risultati sull'esposizione

Security Hub genera risultati sull'esposizione quasi in tempo reale. Man mano che vengono acquisiti nuovi risultati di sicurezza e aggiornati i risultati esistenti, Security Hub genera o aggiorna i risultati sull'esposizione quasi in tempo reale. Security Hub genera un rilevamento dell'esposizione per ID di risorsa.

Security Hub non pubblica i risultati dell'esposizione per tipi di risorse non supportati dai risultati dell'esposizione. Quando una risorsa presenta un numero e una combinazione significativi di caratteristiche, Security Hub genera un risultato di esposizione. Il numero e la combinazione di caratteristiche determinano anche il livello di gravità del risultato dell'esposizione.

Rilevamento dell'esposizione del campione

AWS Security Hub normalizza i risultati di esposizione nell'Open Cybersecurity Schema Framework (OCSF).

Rilevamento dell'esposizione a campioni

Nei seguenti risultati relativi all'esposizione del campione, il `related_events` parametro contiene dettagli esclusivi relativi all'esposizione, come i risultati che contribuiscono all'esposizione. I risultati che contribuiscono sono i tratti e i segnali associati a un dato relativo all'esposizione. Un singolo risultato che contribuisce può includere uno o più tratti. Il `observables` parametro identifica la risorsa associata al risultato che contribuisce. Questo può essere diverso dal `resources` parametro, che identifica la risorsa associata al risultato dell'esposizione.


```
{
    "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"
    }
}
```


Determinazione del livello di gravità di un rilevamento dell'esposizione

AWS Security Hub assegna a ogni esposizione rilevando una gravità predefinita di `CRITICAL`HIGH,`MEDIUM`, o`LOW`. I risultati dell'esposizione con una gravità di non `INFORMATIONAL` sono pubblicati. Security Hub determina la gravità di un rilevamento dell'esposizione combinando due dimensioni, probabilità e impatto, su una matrice di rischio. La probabilità riflette la facilità con cui l'esposizione può essere sfruttata e l'impatto riflette l'entità del danno se viene sfruttato.

Nei casi in cui non è possibile determinare l'impatto su una risorsa, la gravità si basa esclusivamente sulla probabilità.

Matrice del rischio

La tabella seguente mostra come la probabilità e l'impatto si combinano per determinare la gravità finale di un accertamento dell'esposizione. La verosimiglianza stabilisce una gravità di base e l'impatto la aggiusta: un impatto elevato aumenta la gravità di un livello (massimo`CRITICAL`), un impatto medio lascia la gravità invariata e un impatto basso riduce la gravità di un livello (massimo). `INFORMATIONAL` L'impatto regola solo la gravità stabilita dalla probabilità. L'impatto da solo non genera un risultato sull'esposizione.

Matrice di severità e rischio

Probabilità ↓/Impatto →	Bassa	Media	Elevata
Molto alto	HIGH (ELEVATO)	CRITICO	CRITICO
Elevate	MEDIO	HIGH (ELEVATO)	CRITICO

Probabilità ↓/Impatto →	Bassa	Media	Elevata
Moderato	BASSO	MEDIO	HIGH (ELEVATO)
Bassa	INFORMATIVO	BASSO	MEDIO

> **Note**
>
> La bassa probabilità combinata con un basso impatto si traduce in una gravità di`INFORMATIONAL`. Security Hub non pubblica i risultati sull'esposizione con questa gravità, quindi non vengono visualizzati nella pagina Esposizioni o nei GetFindingsV2risultati.

Probabilità

La verosimiglianza misura la facilità con cui un'esposizione può essere sfruttata, in base alle caratteristiche che contribuiscono alla risorsa, ad esempio presupponibilità, errata configurazione, raggiungibilità, dati sensibili e vulnerabilità. Security Hub utilizza diverse caratteristiche per valutare la verosimiglianza, tra cui:

- Consapevolezza: la misura in cui l'esposizione non è teorica, ma presenta exploit disponibili al pubblico o automatizzati.
- Facilità di scoperta: indipendentemente dal fatto che siano disponibili strumenti automatizzati, come la scansione delle porte o la ricerca su Internet, per individuare la risorsa a rischio.
- Facilità di sfruttamento: la facilità con cui un autore di minacce può sfruttare l'esposizione. Ad esempio, se esistono percorsi di rete aperti o metadati configurati in modo errato, un autore della minaccia può sfruttare più facilmente l'esposizione.
- Probabilità di sfruttamento: la probabilità che l'esposizione venga sfruttata nei prossimi 30 giorni. Questo fattore corrisponde all'Exploit Prediction Scoring System (EPSS).

Impatto

L'impatto misura l'entità del danno all'ambiente se l'esposizione viene sfruttata. Ad esempio, un'esposizione potrebbe portare alla perdita di responsabilità, alla perdita di disponibilità, alla perdita di riservatezza derivante dall'esposizione dei dati o alla perdita di integrità dovuta al danneggiamento dei dati.

Per valutare l'impatto, Security Hub analizza le autorizzazioni effettive dei AWS Identity and Access Management principali associati alla risorsa per determinare le azioni che Servizi AWS un utente malintenzionato potrebbe invocare. Identifica inoltre le risorse esistenti che un utente malintenzionato potrebbe raggiungere e compromettere attraverso l'escalation dei privilegi. Per ulteriori informazioni, consulta Impatto e autorizzazioni efficaci.

Revisione dei risultati sull'esposizione

Puoi esaminare tutti i risultati relativi all'esposizione nella console Security Hub e con l'GetFindingsV2API. La pagina Esposizioni nella console Security Hub mostra tutti i risultati dell'esposizione attiva. I risultati dell'esposizione sono elencati in ordine decrescente di gravità. Puoi filtrare i risultati dell'esposizione aggiungendo e rimuovendo filtri con la barra di ricerca Aggiungi filtro. Puoi raggruppare i risultati dell'esposizione con il menu a discesa Raggruppa per. Puoi anche filtrare i risultati dell'esposizione con il menu Filtri rapidi.

Dettagli sui risultati dell'esposizione

È possibile visualizzare molti dettagli relativi ai risultati dell'esposizione. Questi dettagli sono suddivisi tra le schede della console Security Hub. La scheda Panoramica fornisce dettagli chiave sul rilevamento dell'esposizione. La scheda Caratteristiche elenca le caratteristiche e i segnali associati a un rilevamento dell'esposizione. La scheda Risorse fornisce dettagli sulla risorsa e sui tag delle risorse associati a un risultato dell'esposizione. L'elenco seguente fornisce le descrizioni dei dettagli dei risultati relativi all'esposizione.

- Titolo del risultato: il titolo del risultato dell'esposizione.
- Livello di gravità: il livello di gravità del risultato dell'esposizione. Security Hub utilizza il numero e la combinazione di caratteristiche di una risorsa per determinare il livello di gravità di un rilevamento dell'esposizione. Il livello di gravità può essere`CRITICAL`, `HIGH`MEDIUM, o`LOW`. Security Hub non pubblica risultati di esposizione con una gravità di`INFORMATIONAL`. È possibile aggiornarlo `Severity` tramite la console Security Hub o con l'operazione BatchUpdateFindingsV2API.
- Descrizione: la descrizione dei risultati relativi all'esposizione.
- Tipo: il nome del tipo di rilevamento dell'esposizione. Ad esempio, il nome potrebbe essere simile a. `Exposure/Potential Impact/Resource Hijacking`
- Account: l'ID del Account AWS luogo in cui è stato generato il risultato dell'esposizione.
- Età: indica da quanto tempo il risultato dell'esposizione è attivo.
- Ora di creazione: un timestamp che indica quando è stato creato il risultato dell'esposizione.

- Ora modificata: un timestamp che indica quando il risultato dell'esposizione è stato aggiornato l'ultima volta.
- Regione: il Regione AWS luogo in cui è stato generato il risultato dell'esposizione.
- Nome del prodotto: il nome del prodotto che ha generato i risultati sull'esposizione. Questo sarà sempre Security Hub Exposure Detection.
- Nome dell'azienda: il nome della società che ha generato il risultato sull'esposizione. Così sarà sempre AWS.
- Nome dell'attività: il nome dell'ultima attività eseguita rispetto al risultato.
- Stato: lo stato di questo risultato sull'esposizione.
- Finding ID: un identificatore univoco associato al risultato dell'esposizione.
- Percorso di attacco potenziale (solo console): una visualizzazione interattiva che mostra come i potenziali aggressori possono accedere e assumere il controllo delle risorse associate a un rilevamento dell'esposizione. Per ulteriori informazioni, consulta Visualizzazione delle esposizioni in Security Hub con il grafico del percorso del potenziale attacco.
- Caratteristiche: identifica i tipi di caratteristiche e i titoli delle caratteristiche associati al risultato dell'esposizione. Nella console Security Hub, puoi visualizzare le caratteristiche per tipo di caratteristica o segnale. Ciò consente di analizzare i risultati che contribuiscono al contesto della relativa esposizione.
- Correzione: collegamenti alla documentazione di correzione specifica per le caratteristiche identificate nell'esposizione.
- Risorse: identifica la risorsa associata alla rilevazione dell'esposizione.

Revisione dei dettagli relativi ai risultati dell'esposizione

Questo argomento descrive come esaminare i dettagli sui risultati dell'esposizione nella console AWS Security Hub e con l'API.

Esame dei dettagli relativi a un rilevamento dell'esposizione nella console Security Hub

Per visualizzare i dettagli di un rilevamento dell'esposizione nella console Security Hub

1. Accedi utilizzando le tue credenziali e apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal pannello di navigazione, scegli Esposizioni.
3. Scegliete un'esposizione di cui desiderate visualizzare i dettagli.

Analisi dei dettagli relativi a un risultato dell'esposizione con l'API

Puoi esaminare i risultati dell'esposizione con l'GetFindingsV2API o con AWS CLI. Puoi filtrare tutti i risultati dell'esposizione con il `metadata.product.feature.uid` campo con il `security-hub/Exposure` valore. Per ulteriori informazioni, consulta GetFindingsV2.

Esempio di comando

Di seguito è riportato un AWS CLI esempio che recupera i 10 risultati di esposizione generati più di recente nel tuo account. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

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

Visualizzazione delle esposizioni in Security Hub con il grafico del percorso del potenziale attacco

Il grafico del percorso di attacco potenziale è una visualizzazione interattiva che mostra come i potenziali aggressori possono accedere e assumere il controllo delle risorse associate a un rilevamento dell'esposizione. È possibile accedere a questo grafico solo nella console Security Hub dalla pagina Esposizioni. Quando si visualizzano i dettagli di un risultato di esposizione, la scheda Panoramica include una sezione chiamata Potential attack path e Blast radius.

Il grafico del percorso di attacco mostra la risorsa principale da cui è stata generata l'esposizione, il percorso di rete (se applicabile) e le risorse a valle che un aggressore potrebbe raggiungere aumentando le autorizzazioni. Quando Security Hub identifica percorsi concreti di escalation dei privilegi dalla risorsa principale ad altre risorse dell'ambiente, li visualizza come parte del grafico relativa al raggio di esplosione. Ogni nodo rappresenta una risorsa e le connessioni tra i nodi mostrano le autorizzazioni che consentono a un utente malintenzionato di passare da una risorsa all'altra.

In questa sezione della scheda Panoramica, puoi scegliere e trascinare AWS le risorse nel grafico del potenziale percorso di attacco. Puoi concentrarti su aree specifiche del grafico del percorso di attacco con le icone di ingrandimento e riduzione. Puoi espandere il grafico del percorso di attacco

attivando e disattivando la modalità a schermo intero tramite l'icona a schermo intero. La legenda codifica la risorsa principale, la risorsa coinvolta, le risorse del raggio d'esplosione e il conteggio delle caratteristiche che contribuiscono al conteggio per colore e mostra le categorie di caratteristiche e il numero di caratteristiche nel grafico del percorso di attacco. È possibile visualizzare i dettagli di una risorsa selezionando una risorsa e selezionando Visualizza i dettagli della risorsa. Puoi anche copiare l'ID e il Account AWS numero associati a una risorsa. I risultati dell'esposizione con una caratteristica di raggiungibilità mostrano la rete Internet pubblica e il percorso di rete compresso nel grafico del percorso di attacco. È possibile visualizzare questi dettagli scegliendo il nodo del percorso di rete compresso.

Per visualizzare le risorse a valle e i percorsi di assegnazione dei privilegi che le collegano, scegli la scheda Valutazione dell'impatto. Ogni percorso mostra la catena di risorse che un utente malintenzionato potrebbe attraversare e le autorizzazioni specifiche per ogni fase. Per ulteriori informazioni sulle caratteristiche di impatto e sulle autorizzazioni effettive, consulta. Impatto e autorizzazioni efficaci

Correzione dei risultati dell'esposizione

Gli argomenti di questa sezione descrivono le fasi di correzione dei risultati dell'esposizione in diversi settori. Servizi AWS

Il `Remediation` campo del formato OCSF contiene due campi: e. `remediation` `references`

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

> **Note**
>
> Le linee guida sulla riparazione fornite nelle sezioni seguenti potrebbero richiedere ulteriori consultazioni in altre risorse. AWS

Correzione delle esposizioni per le tabelle DynamoDB

AWS Security Hub può generare risultati sull'esposizione per le tabelle DynamoDB.

Nella console Security Hub, la tabella DynamoDB coinvolta nella rilevazione dell'esposizione e le relative informazioni identificative sono elencate nella sezione Risorse dei dettagli dei risultati. A livello di programmazione, è possibile recuperare i dettagli delle risorse con il GetFindingsV2 funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la risoluzione fornite in questo argomento potrebbero richiedere ulteriori consultazioni in altre risorse. AWS

Indice

- Caratteristiche di configurazione errata in DynamoDB
  - La tabella DynamoDB ha il ripristino point-in-time disabilitato
  - La tabella DynamoDB non è coperta da un piano di backup
  - La protezione dalle cancellazioni nella tabella DynamoDB è disattivata

Caratteristiche di configurazione errata in DynamoDB

Di seguito vengono descritte le caratteristiche di configurazione errata e le fasi di correzione per le tabelle DynamoDB.

La tabella DynamoDB ha il ripristino point-in-time disabilitato

Correzione: abilita il ripristino point-in-time di DynamoDB

Il ripristino point-in-time di DynamoDB fornisce backup automatici continui per i dati delle tabelle DynamoDB. Per informazioni su come ripristinare una tabella DynamoDB in un punto temporale, consulta Restoring a DynamoDB table to a point in time nella Amazon DynamoDB Developer Guide.

La tabella DynamoDB non è coperta da un piano di backup

AWS Backup fornisce un servizio centralizzato per configurare, gestire e automatizzare i backup su tutti AWS i servizi, incluso DynamoDB. Senza un piano di backup, la tabella non dispone di backup pianificati e automatici con periodi di conservazione personalizzabili, il che comporta rischi significativi per la sicurezza. Un utente malintenzionato potrebbe danneggiare o eliminare dolosamente i dati della tabella. Senza backup adeguati, potresti non avere alcuna opzione di ripristino oltre la finestra di Point-in-Time ripristino (se abilitata), con conseguente potenziale perdita permanente dei dati. Seguendo le best practice per la protezione dei dati, coprite le tabelle DynamoDB con un piano di backup.

Correzione: crea un piano di backup

Prima di creare un piano di backup, stabilisci la frequenza di backup e i periodi di conservazione appropriati per i tuoi dati. Per informazioni su come creare un piano di backup, consulta Assegnare risorse a un piano di backup nella AWS Backup Developer Guide.

La protezione dalle cancellazioni nella tabella DynamoDB è disattivata

La protezione dall'eliminazione impedisce l'eliminazione accidentale delle tabelle DynamoDB. Quando la protezione dalle eliminazioni è disabilitata, le tabelle DynamoDB sono vulnerabili all'eliminazione involontaria tramite azioni della console, chiamate API, comandi CLI o processi automatizzati. Ciò può esporre AWS l'ambiente alla perdita di dati, in quanto un'entità non autorizzata con accesso all' AWS ambiente potrebbe eliminare intenzionalmente le tabelle, con conseguente interruzione del servizio e perdita permanente dei dati. Seguendo le best practice di protezione dei dati, abilita la protezione dei dati per le tabelle DynamoDB.

Correzione: abilita la protezione dalle cancellazioni

Se gestisci più tabelle, valuta la possibilità di CloudFormation aggiornare le proprietà delle tabelle in blocco. Puoi modificare i tuoi CloudFormation modelli per includere `DeletionProtectionEnabled` proprietà e aggiornare i tuoi stack. Dopo aver completato la correzione, verifica che la protezione dall'eliminazione sia abilitata nel menu a discesa Informazioni aggiuntive nella scheda Impostazioni della tabella.

Riparazione delle esposizioni per le istanze EC2

AWS Security Hub può generare risultati sull'esposizione per le istanze Amazon Elastic Compute Cloud (EC2).

Sulla console Security Hub, l'istanza EC2 coinvolta in un rilevamento dell'esposizione e le relative informazioni identificative sono elencate nella sezione Risorse dei dettagli del risultato. A livello di codice, è possibile recuperare i dettagli delle risorse con il GetFindingsV2funzionamento dell'API CSPM Security Hub.

Dopo aver identificato la risorsa coinvolta in un rilevamento dell'esposizione, puoi eliminare la risorsa se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per mitigare il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato sull'esposizione contiene i problemi identificati in diversi argomenti relativi alla correzione. Al contrario, è possibile risolvere un problema di esposizione e ridurne il livello di gravità affrontando un solo argomento di correzione. L'approccio alla risoluzione dei rischi dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida sulla correzione fornite in questo argomento potrebbero richiedere ulteriori consultazioni in altre risorse. AWS

Indice

- Caratteristiche di errata configurazione per le istanze EC2
  - L'istanza EC2 consente l'accesso a IMDS utilizzando la versione 1
  - L'istanza Amazon EC2 ha un gruppo di sicurezza o un ACL di rete che consente l'accesso SSH o RDP.
  - L'istanza Amazon EC2 ha un gruppo di sicurezza aperto
- Caratteristiche di raggiungibilità per le istanze EC2
  - L'istanza EC2 è raggiungibile tramite Internet
- Caratteristiche di vulnerabilità per le istanze EC2
  - L'istanza EC2 presenta vulnerabilità software sfruttabili in rete con un'elevata probabilità di sfruttamento
  - L'istanza Amazon EC2 presenta vulnerabilità software
  - L'istanza EC2 ha un sistema operativo End-Of-Life
  - L'istanza EC2 contiene pacchetti software dannosi

  - L'istanza EC2 contiene file dannosi
- Caratteristiche di impatto per le istanze EC2
  - Dispone di un percorso di esecutore privilegiato con pieno controllo
  - Ha un percorso diretto di escalation delle politiche
  - Dispone di un percorso di dirottamento delle politiche di fiducia
  - Ha un percorso di ransomware per i dati
  - Ha un percorso di rimozione della restrizione
  - Ha il percorso pass role create executor
  - Ha un percorso di esecuzione esistente di Swap Role
  - Ha un percorso di escalation della catena di ruoli
  - Dispone di un percorso di esecutore privilegiato per il codice di iniezione
  - Ha disabilitato il percorso di audit trail
  - Ha accesso al percorso dell'esecutore esistente
  - Dispone di un percorso di coniazione delle credenziali
  - Dispone di un percorso di accesso ai dati di accesso ai dati
  - Ha un percorso di dirottamento del ruolo
  - Dispone di un percorso di accesso ai dati a hop singolo
  - Ha un percorso di avanzamento delle capacità
  - Criticità aziendale

Caratteristiche di errata configurazione per le istanze EC2

Ecco le caratteristiche di configurazione errata per le istanze EC2 e le procedure di correzione suggerite.

L'istanza EC2 consente l'accesso a IMDS utilizzando la versione 1

I metadati dell'istanza sono dati sull'istanza Amazon EC2 che le applicazioni possono utilizzare per configurare o gestire l'istanza in esecuzione. Il servizio di metadati dell'istanza (IMDS) è un componente dell'istanza utilizzato dal codice sull'istanza per accedere in modo sicuro ai metadati dell'istanza. Se l'IMDS non è adeguatamente protetto, può diventare un potenziale vettore di attacco, in quanto fornisce l'accesso a credenziali temporanee e ad altri dati di configurazione sensibili. IMDSv2 offre una protezione più forte contro lo sfruttamento attraverso l'autenticazione orientata alla sessione, che richiede un token di sessione per le richieste di metadati e limita la durata della

sessione. Seguendo i principi di sicurezza standard, configura le istanze Amazon EC2 per utilizzare IMDSv2 e disabilitare IMDSv1.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Verifica la compatibilità delle applicazioni

Prima di implementare IMDSv2, verifica la tua istanza per assicurarne la compatibilità con IMDSv2. Alcune applicazioni o script potrebbero richiedere IMDSv1 per le funzionalità di base e richiedere una configurazione aggiuntiva. Per ulteriori informazioni sugli strumenti e sui percorsi consigliati per testare la compatibilità delle applicazioni, consulta la Transizione all'utilizzo di Instance Metadata Service versione 2 nella Amazon Elastic Compute Cloud User Guide.

Aggiorna l'istanza per utilizzare IMDSv2

Modifica le istanze esistenti per utilizzare IMDSv2. Per ulteriori informazioni, consulta Modificare le opzioni dei metadati delle istanze per le istanze esistenti nella Amazon Elastic Compute Cloud User Guide.

Applica aggiornamenti alle istanze in un gruppo di Auto Scaling

Se la tua istanza fa parte di un gruppo Auto Scaling, aggiorna il modello di lancio o la configurazione di avvio con una nuova configurazione ed esegui un aggiornamento dell'istanza.

L'istanza Amazon EC2 ha un gruppo di sicurezza o un ACL di rete che consente l'accesso SSH o RDP.

I protocolli di accesso remoto come SSH e RDP consentono agli utenti di connettersi e gestire istanze Amazon EC2 da postazioni esterne. Quando i gruppi di sicurezza consentono l'accesso illimitato a questi protocolli da Internet, aumentano la superficie di attacco delle istanze Amazon EC2 consentendo l'accesso a Internet all'istanza. Seguendo i principi di sicurezza standard, limita l'accesso remoto a indirizzi o intervalli IP specifici e affidabili.

Correzione: modifica delle regole del gruppo di sicurezza

Limita l'accesso alle tue istanze Amazon EC2 a indirizzi IP affidabili specifici. Limita l'accesso SSH e RDP a specifici indirizzi IP affidabili o usa la notazione CIDR per specificare gli intervalli IP (ad esempio, 192.168.1). 0/24). Per modificare le regole dei gruppi di sicurezza, consulta Configura le regole dei gruppi di sicurezza nella Amazon Elastic Compute Cloud User Guide.

L'istanza Amazon EC2 ha un gruppo di sicurezza aperto

I gruppi di sicurezza fungono da firewall virtuali per le istanze Amazon EC2 per controllare il traffico in entrata e in uscita. I gruppi di sicurezza aperti, che consentono l'accesso illimitato da qualsiasi indirizzo IP, possono esporre le istanze ad accessi non autorizzati. Seguendo i principi di sicurezza standard, limita l'accesso dei gruppi di sicurezza a indirizzi IP e porte specifici.

Correzione

Esegui una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi le regole del gruppo di sicurezza e valuta la configurazione corrente

Valuta quali porte sono aperte e accessibili da ampi intervalli IP, ad esempio(`0.0.0.0/0 or ::/0`). Per istruzioni sulla visualizzazione dei dettagli dei gruppi di sicurezza, consulta DescribeSecurityGroupsil Porting Assistant for .NET API Reference.

Modifica le regole del gruppo di sicurezza

Modifica le regole del gruppo di sicurezza per limitare l'accesso a intervalli o indirizzi IP affidabili specifici. Quando aggiorni le regole del gruppo di sicurezza, prendi in considerazione la possibilità di separare i requisiti di accesso per i diversi segmenti di rete creando regole per ogni intervallo IP di origine richiesto o limitando l'accesso a porte specifiche. Per modificare le regole dei gruppi di sicurezza, consulta Configura le regole dei gruppi di sicurezza nella Guida per l'utente di Amazon EC2.

Caratteristiche di raggiungibilità per le istanze EC2

Di seguito sono riportati i tratti di raggiungibilità per le istanze EC2 e le procedure di correzione suggerite.

L'istanza EC2 è raggiungibile tramite Internet

Le istanze Amazon EC2 con porte raggiungibili da Internet potrebbero esporre la tua istanza. La raggiungibilità può avvenire tramite un gateway Internet (incluse le istanze di Application Load Balancer o Classic Load Balancer), una connessione peering VPC o un gateway virtuale VPN. Seguendo i principi di sicurezza standard, implementa controlli di accesso alla rete con privilegi minimi limitando il traffico in entrata solo alle sorgenti e alle porte necessarie.

Correzione

Intraprendi una o più delle seguenti azioni per ovviare a questa esposizione:

Modifica o rimuovi le regole dei gruppi di sicurezza

Nella scheda Risorse, apri la risorsa per il gruppo di sicurezza Amazon EC2. Verifica se è necessario l'accesso a Internet per il funzionamento dell'istanza. Modifica o rimuovi le regole dei gruppi di sicurezza in entrata che consentono l'accesso illimitato (`0.0.0.0/0`o`::/0`). Implementa regole più restrittive basate su intervalli IP o gruppi di sicurezza specifici. Se è necessario un accesso pubblico limitato, limita l'accesso a porte e protocolli specifici necessari per la funzione dell'istanza. Per istruzioni sulla gestione delle regole dei gruppi di sicurezza, consulta Configura le regole dei gruppi di sicurezza nella Guida per l'utente di Amazon EC2.

Aggiorna gli ACL di rete

Rivedi e modifica gli elenchi di controllo degli accessi alla rete (ACL) associati alla sottorete dell'istanza. Verifica che le impostazioni ACL siano in linea con le modifiche del gruppo di sicurezza e non consentano involontariamente l'accesso pubblico. Per istruzioni sulla modifica degli ACL di rete, consulta Lavorare con gli ACL di rete nella Amazon VPC User Guide.

Metodi di accesso alternativi

Considerate le seguenti opzioni per metodi di accesso alternativi:

- Usa NAT Gateway per la connettività Internet in uscita: per esempio in sottoreti private che richiedono l'accesso a Internet (ad esempio, per scaricare gli aggiornamenti), prendi in considerazione l'utilizzo di un gateway NAT anziché assegnare un indirizzo IP pubblico. Un gateway NAT consente alle istanze in sottoreti private di avviare connessioni in uscita a Internet impedendo al contempo le connessioni in entrata da Internet.
- Usa Systems Manager Session Manager: Session Manager fornisce un accesso sicuro alla shell alle istanze Amazon EC2 senza la necessità di porte in ingresso, gestione di chiavi SSH o manutenzione di host bastion.
- Usa WAF ed Elastic Load Balancing o Application Load Balancer: per le istanze che eseguono applicazioni Web, prendi in considerazione l'utilizzo di un LB AWS combinato con Web Application Firewall (WAF). I LB possono essere configurati per consentire l'esecuzione delle istanze in sottoreti private mentre il LB viene eseguito in una sottorete pubblica e gestisce il traffico Internet. L'aggiunta di un WAF al sistema di bilanciamento del carico offre una protezione aggiuntiva contro gli exploit Web e i bot.

Caratteristiche di vulnerabilità per le istanze EC2

Di seguito sono riportati i tratti di vulnerabilità delle istanze EC2 e le procedure di correzione suggerite.

L'istanza EC2 presenta vulnerabilità software sfruttabili in rete con un'elevata probabilità di sfruttamento

I pacchetti software installati sulle istanze EC2 possono essere esposti a vulnerabilità ed esposizioni comuni (CVE). I CVE critici rappresentano rischi significativi per la sicurezza dell'ambiente. AWS I responsabili non autorizzati possono sfruttare queste vulnerabilità prive di patch per compromettere la riservatezza, l'integrità o la disponibilità dei dati o per accedere ad altri sistemi. Le vulnerabilità critiche con un'elevata probabilità di sfruttamento rappresentano minacce immediate alla sicurezza, poiché il codice di exploit potrebbe già essere disponibile al pubblico e utilizzato attivamente dagli aggressori o dagli strumenti di scansione automatizzati. Correggi queste vulnerabilità per proteggere la tua istanza.

Correzione: aggiorna le istanze interessate

Esamina la sezione Riferimenti nella scheda Vulnerabilità della caratteristica. La documentazione del fornitore può includere linee guida specifiche per la correzione. Segui la correzione appropriata utilizzando queste linee guida generali:

Usa Systems Manager Patch Manager per applicare le patch sia per i sistemi operativi che per le applicazioni. Patch Manager consente di selezionare e distribuire automaticamente le patch del sistema operativo e del software su grandi gruppi di istanze. Se Patch Manager non è configurato, aggiorna manualmente il sistema operativo su ogni istanza interessata.

Aggiorna le applicazioni interessate alle versioni sicure più recenti seguendo le procedure consigliate dal fornitore. Per gestire gli aggiornamenti delle applicazioni su più istanze, prendete in considerazione l'utilizzo di Systems Manager State Manager per mantenere il software in uno stato coerente. Se gli aggiornamenti non sono disponibili, prendete in considerazione la possibilità di rimuovere o disabilitare l'applicazione vulnerabile fino al rilascio di una patch o di adottare altre misure di mitigazione, come la limitazione dell'accesso alla rete all'applicazione o la disabilitazione delle funzionalità vulnerabili.

Segui i consigli di riparazione specifici forniti nei risultati di Amazon Inspector. Ciò potrebbe comportare la modifica delle regole dei gruppi di sicurezza, la modifica delle configurazioni delle istanze o la regolazione delle impostazioni dell'applicazione.

Controlla se l'istanza fa parte di Auto Scaling Group. AMI-replacement l'applicazione di patch viene eseguita su infrastrutture immutabili aggiornando l'ID AMI configurato per distribuire nuove istanze Amazon EC2 in un gruppo Auto Scaling. Se utilizzi un' custom/golden AMI, crea un'istanza con la nuova AMI, quindi personalizza l'istanza e crea una nuova AMI dorata. Per ulteriori informazioni, vedi Applicazione delle patch agli aggiornamenti AMI (utilizzo delle AMI patchate per i gruppi di Auto Scaling).

Considerazioni future

Per prevenire situazioni future, prendi in considerazione l'implementazione di un programma di gestione delle vulnerabilità. Amazon Inspector può essere configurato per eseguire automaticamente la scansione dei CVE sulle istanze. Amazon Inspector può anche essere integrato con Security Hub per le riparazioni automatiche. Prendi in considerazione l'implementazione di una pianificazione regolare delle patch utilizzando Systems Manager Maintenance Windows per ridurre al minimo le interruzioni delle istanze.

L'istanza Amazon EC2 presenta vulnerabilità software

I pacchetti software installati sulle istanze Amazon EC2 possono essere esposti a vulnerabilità ed esposizioni comuni (CVE). I CVE non critici rappresentano punti deboli di sicurezza con gravità o sfruttabilità inferiori rispetto ai CVE critici. Sebbene queste vulnerabilità rappresentino un rischio meno immediato, gli aggressori possono comunque sfruttare queste vulnerabilità prive di patch per compromettere la riservatezza, l'integrità o la disponibilità dei dati o per accedere ad altri sistemi. Seguendo le best practice di sicurezza, correggi queste vulnerabilità per proteggere la tua istanza dagli attacchi.

Correzione: aggiorna le istanze interessate

Usa AWS Systems Manager Patch Manager per applicare le patch ai sistemi operativi. Patch Manager consente di selezionare e distribuire automaticamente le patch del sistema operativo e del software su grandi gruppi di istanze. Se Patch Manager non è configurato, aggiorna manualmente il sistema operativo su ogni istanza interessata.

Aggiorna le applicazioni interessate alle versioni sicure più recenti seguendo le procedure consigliate dal fornitore. Per gestire gli aggiornamenti delle applicazioni su più istanze, prendete in considerazione l'utilizzo di AWS Systems Manager State Manager per mantenere il software in uno stato coerente. Se gli aggiornamenti non sono disponibili, prendete in considerazione la possibilità di rimuovere o disabilitare l'applicazione vulnerabile fino al rilascio di una patch o di adottare altre misure di mitigazione, come la limitazione dell'accesso alla rete all'applicazione o la disabilitazione delle funzionalità vulnerabili.

Segui i consigli di riparazione specifici forniti nei risultati di Amazon Inspector. Ciò potrebbe comportare la modifica delle regole dei gruppi di sicurezza, la modifica delle configurazioni delle istanze o la regolazione delle impostazioni dell'applicazione.

Controlla se l'istanza fa parte di Auto Scaling Group. AMI-replacement l'applicazione di patch viene eseguita su infrastrutture immutabili aggiornando l'ID AMI configurato per distribuire nuove istanze Amazon EC2 in un gruppo Auto Scaling. Se utilizzi un' custom/golden AMI, crea un'istanza con la nuova AMI, quindi personalizza l'istanza e crea una nuova AMI dorata. Per ulteriori informazioni, vedi Applicazione delle patch agli aggiornamenti AMI (utilizzo delle AMI patchate per i gruppi di Auto Scaling).

Considerazioni future

Per prevenire situazioni future, prendi in considerazione l'implementazione di un programma di gestione delle vulnerabilità. Amazon Inspector può essere configurato per eseguire automaticamente la scansione dei CVE sulle istanze. Amazon Inspector può anche essere integrato con Security Hub per le riparazioni automatiche. Prendi in considerazione l'implementazione di una pianificazione regolare delle patch utilizzando Systems Manager Maintenance Windows per ridurre al minimo le interruzioni delle istanze.

L'istanza EC2 ha un sistema operativo End-Of-Life

L'istanza EC2 esegue un sistema operativo scaduto che non è più supportato o gestito dallo sviluppatore originale. Ciò espone l'istanza a vulnerabilità di sicurezza e potenziali attacchi. Quando i sistemi operativi raggiungono la fine del ciclo di vita, i fornitori in genere smettono di rilasciare nuovi avvisi di sicurezza. Gli avvisi di sicurezza esistenti possono anche essere rimossi dai feed dei fornitori. Di conseguenza, Amazon Inspector potrebbe potenzialmente smettere di generare risultati per CVE noti, creando ulteriori lacune nella copertura di sicurezza.

Consulta i sistemi operativi fuori produzione nella Amazon Inspector User Guide per informazioni sui sistemi operativi che hanno raggiunto la fine del ciclo di vita che possono essere rilevati da Amazon Inspector.

Correzione: aggiornamento a una versione del sistema operativo supportata

Aggiornamento a una versione supportata del sistema operativo. Nel risultato dell'esposizione, aprite la risorsa per accedere alla risorsa interessata. Prima di aggiornare la versione del sistema operativo sull'istanza, crea un'istantanea o un backup AMI nel caso in cui sia necessario eseguire il rollback. Quindi, consulta le versioni disponibili in Supported Operating Systems nella Amazon Inspector User Guide per un elenco delle versioni del sistema operativo attualmente supportate.

L'istanza EC2 contiene pacchetti software dannosi

I pacchetti dannosi sono componenti software che contengono codice dannoso progettato per compromettere la riservatezza, l'integrità e la disponibilità dei sistemi e dei dati. I pacchetti dannosi rappresentano una minaccia attiva e critica per l'istanza, in quanto gli aggressori possono eseguire codice dannoso automaticamente senza sfruttare una vulnerabilità. Seguendo le best practice di sicurezza, rimuovi i pacchetti dannosi per proteggere l'istanza da potenziali attacchi.

Correzione: rimuovi i pacchetti dannosi

Esamina i dettagli del pacchetto dannoso nella sezione Riferimenti della scheda Vulnerabilità della caratteristica per comprendere la minaccia. Rimuovi i pacchetti dannosi identificati utilizzando il gestore di pacchetti appropriato. Per un esempio, consulta lo strumento di gestione dei pacchetti nella Guida per l'utente di Amazon Linux 2023. Dopo aver rimosso i pacchetti dannosi, valuta la possibilità di eseguire una scansione per verificare che tutti i pacchetti che potrebbero essere stati installati dal codice dannoso siano stati rimossi. Per ulteriori informazioni, consulta Avvio della scansione On-demand antimalware GuardDuty in.

L'istanza EC2 contiene file dannosi

I file dannosi contengono codice dannoso progettato per compromettere la riservatezza, l'integrità e la disponibilità dei sistemi e dei dati. I file dannosi rappresentano una minaccia attiva e critica per l'istanza, in quanto gli aggressori possono eseguire codice dannoso automaticamente senza sfruttare una vulnerabilità. Seguendo le best practice di sicurezza, rimuovi i file dannosi per proteggere l'istanza da potenziali attacchi.

Correzione: rimuovi i file dannosi

Per identificare lo specifico volume Amazon Elastic Block Store (Amazon EBS) che contiene file dannosi, consulta la sezione Risorse dei dettagli relativi alla scoperta della caratteristica. Dopo aver identificato il volume con il file dannoso, crea un'istantanea del volume prima di apportare modifiche, quindi rimuovi i file dannosi identificati. Dopo aver rimosso i file dannosi, valuta la possibilità di eseguire una scansione per verificare che tutti i file che potrebbero essere stati installati dal file dannoso siano stati rimossi. Per ulteriori informazioni, consulta Avvio della scansione On-demand antimalware GuardDuty in.

Caratteristiche di impatto per le istanze EC2

Le caratteristiche di impatto descrivono il potenziale raggio di esplosione di un'esposizione. Security Hub analizza le autorizzazioni effettive del AWS Identity and Access Management principale

associato all'istanza EC2 per determinare le risorse a valle che un utente malintenzionato potrebbe raggiungere se l'istanza viene compromessa, nonché la criticità aziendale di tali risorse. Ogni caratteristica di impatto identifica uno specifico modello di escalation dei privilegi. Per ridurre il raggio d'azione, esaminate i percorsi di autorizzazione descritti in ogni caratteristica e rimuovete eventuali privilegi non necessari.

Seguendo i principi di sicurezza standard, concedi il privilegio minimo fornendo solo le autorizzazioni necessarie per eseguire un'attività. Sostituisci politiche generali con politiche circoscritte che garantiscano solo le azioni e le risorse specifiche necessarie. Per identificare le autorizzazioni non utilizzate da rimuovere, utilizza IAM Access Analyzer per generare consigli basati sulla cronologia degli accessi. Per ulteriori informazioni, consulta Findings for external and inused access e Apply least-privilege permissions nella IAM User Guide.

Dispone di un percorso di esecutore privilegiato con pieno controllo

Il principale associato può passare un ruolo e inserire codice in una risorsa di calcolo che dispone già di autorizzazioni elevate. Ciò consente al principale di ottenere il pieno controllo sull'esecutore ed eseguire qualsiasi azione consentita dal ruolo dell'esecutore.

Ha un percorso diretto di escalation delle politiche

Il principale associato può modificare direttamente le politiche IAM per concedersi autorizzazioni aggiuntive, aumentando i propri privilegi senza risorse intermedie.

Dispone di un percorso di dirottamento delle politiche di fiducia

Il principale associato può modificare la politica di fiducia di un ruolo IAM per consentirsi di assumere quel ruolo, ottenendo le autorizzazioni del ruolo.

Ha un percorso di ransomware per i dati

Il principale associato può crittografare o eliminare i dati in un modo che potrebbe essere utilizzato per il ransomware, ad esempio crittografando gli oggetti Amazon S3 con una AWS KMS chiave gestita dal cliente e quindi modificando la politica della chiave.

Ha un percorso di rimozione della restrizione

Il principale associato può rimuovere le restrizioni di sicurezza come i limiti di autorizzazione, le politiche di controllo dei servizi o le dichiarazioni di rifiuto delle politiche basate sulle risorse, ampliando le funzionalità che possono fare gli altri principali o la risorsa stessa.

Ha il percorso pass role create executor

Il principale associato può creare una nuova risorsa di calcolo (come una funzione Lambda o un'istanza Amazon EC2) e assegnarle un ruolo privilegiato, riciclando efficacemente le proprie autorizzazioni attraverso la nuova risorsa.

Ha un percorso di esecuzione esistente di Swap Role

Il principale associato può modificare il ruolo IAM associato a una risorsa di elaborazione esistente, sostituendolo con un ruolo più privilegiato per aumentare l'accesso.

Ha un percorso di escalation della catena di ruoli

Il principale associato può assumere una sequenza di ruoli, in cui ogni ruolo della catena dispone di autorizzazioni progressivamente più ampie, fino a raggiungere infine un ruolo altamente privilegiato.

Dispone di un percorso di esecutore privilegiato per il codice di iniezione

Il principale associato può iniettare codice in una risorsa di elaborazione in esecuzione che dispone di autorizzazioni elevate, eseguendo operazioni arbitrarie nell'ambito del ruolo privilegiato di tale risorsa.

Ha disabilitato il percorso di audit trail

Il responsabile associato può disabilitare i servizi di registrazione o monitoraggio CloudTrail, ad esempio coprire efficacemente le tracce durante o dopo un'escalation.

Ha accesso al percorso dell'esecutore esistente

Il principale associato può richiamare o connettersi a una risorsa di elaborazione esistente e utilizzare il ruolo associato per eseguire azioni privilegiate.

Dispone di un percorso di coniazione delle credenziali

Il principale associato può creare nuove credenziali a lungo termine (come chiavi di accesso o profili di accesso) per altri principali, stabilendo percorsi di accesso persistenti che sopravvivono alla rotazione delle password o alle scadenze delle sessioni.

Dispone di un percorso di accesso ai dati di accesso ai dati

Il responsabile associato può creare una risorsa di servizio e assegnarle un ruolo con accesso a dati sensibili, ottenendo l'accesso indiretto a tali dati tramite la nuova risorsa.

Ha un percorso di dirottamento del ruolo

Il principale associato può passare un ruolo a un'attività pianificata o basata su eventi (come una funzione Lambda attivata da un evento), consentendogli di eseguire codice arbitrario con le autorizzazioni di quel ruolo.

Dispone di un percorso di accesso ai dati a hop singolo

Il principale associato può accedere direttamente alle risorse di dati sensibili (come i bucket Amazon S3 o le tabelle DynamoDB) tramite le autorizzazioni esistenti, senza bisogno di passaggi di escalation intermedi.

Ha un percorso di avanzamento delle capacità

Il principale associato dispone di un percorso di assegnazione dei privilegi che ne migliora le capacità complessive oltre a quanto suggerirebbe l'assegnazione diretta delle autorizzazioni. Questa è una classificazione generale per i percorsi che non corrispondono a uno schema più specifico.

Criticità aziendale

La criticità aziendale della risorsa principale, stabilita dalle regole di automazione o dall'inferenza del nome e dei tag.

Correzione delle esposizioni per i servizi Amazon ECS

AWS Security Hub può generare risultati sull'esposizione per i servizi Amazon Elastic Container Service (Amazon ECS).

Il servizio Amazon ECS coinvolto in un rilevamento dell'esposizione e le relative informazioni identificative sono elencati nella sezione Risorse dei dettagli del risultato. È possibile recuperare questi dettagli delle risorse sulla console di Security Hub o a livello di codice con il GetFindingsV2funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta in un rilevamento dell'esposizione, puoi eliminare la risorsa se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per mitigare il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato sull'esposizione contiene i problemi identificati in diversi argomenti relativi alla correzione. Al contrario, è possibile risolvere un problema di esposizione e ridurne il livello di gravità

affrontando un solo argomento di correzione. L'approccio alla risoluzione dei rischi dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida sulla correzione fornite in questo argomento potrebbero richiedere ulteriori consultazioni in altre risorse. AWS

Indice

- Caratteristiche di configurazione errate per i servizi Amazon ECS
  - Il servizio Amazon ECS utilizza una definizione di attività che consente ai contenitori di accedere ai file system root.
  - Il servizio Amazon ECS utilizza una definizione di attività configurata per condividere lo spazio dei nomi di processo di un host.
  - Il servizio Amazon ECS utilizza una definizione di attività configurata con credenziali in chiaro nelle variabili di ambiente.
  - Il servizio Amazon ECS ha un gruppo di sicurezza aperto
  - Il servizio Amazon ECS dispone di indirizzi IP pubblici
  - Il servizio Amazon ECS utilizza una definizione di attività configurata con la modalità di rete host abilitata.
- Caratteristiche di raggiungibilità per i servizi Amazon ECS
  - Il servizio Amazon ECS è raggiungibile tramite Internet
- Caratteristiche di vulnerabilità per i servizi Amazon ECS
  - Il servizio Amazon ECS dispone di un contenitore con vulnerabilità software sfruttabili in rete con un'elevata probabilità di sfruttamento
  - Il servizio Amazon ECS dispone di un contenitore con vulnerabilità software
  - Il servizio Amazon ECS dispone di un contenitore con un End-Of-Life sistema operativo
  - Il servizio Amazon ECS dispone di un contenitore con pacchetti software dannosi
- Caratteristiche di impatto per i servizi Amazon ECS
  - Dispone del percorso di esecutore privilegiato con pieno controllo
  - Ha un percorso diretto di escalation delle politiche
  - Ha un percorso di dirottamento delle politiche di fiducia

- Ha un percorso di ransomware per i dati
- Ha un percorso di rimozione della restrizione
- Ha il percorso pass role create executor
- Ha un percorso di esecuzione esistente di Swap Role
- Ha un percorso di escalation della catena di ruoli
- Dispone di un percorso di esecuzione privilegiato per il codice di iniezione
- Ha disabilitato il percorso di audit trail
- Ha accesso al percorso dell'esecutore esistente
- Dispone di un percorso di coniazione delle credenziali
- Dispone di un percorso di accesso ai dati di accesso ai dati
- Ha un percorso pass role task hijack
- Ha un percorso di accesso ai dati a hop singolo
- Ha un percorso di avanzamento delle capacità
- Criticità aziendale

Caratteristiche di configurazione errate per i servizi Amazon ECS

Di seguito sono riportate le caratteristiche di errata configurazione dei servizi Amazon ECS e le procedure di correzione suggerite.

Il servizio Amazon ECS utilizza una definizione di attività che consente ai contenitori di accedere ai file system root.

I contenitori Amazon ECS con accesso al filesystem root dell'host possono potenzialmente leggere, modificare o eseguire file critici sul sistema host. Questa configurazione aumenta il rischio che un contenitore compromesso possa essere utilizzato per accedere o modificare risorse al di fuori dell'ambito previsto, esponendo potenzialmente dati sensibili sul file system host. Seguendo i principi di sicurezza standard, concedi i privilegi minimi, il che significa che concedi solo le autorizzazioni necessarie per eseguire un'attività.

Correzione: revisione e modifica dei contenitori con accesso al file system host

Nel rilevamento dell'esposizione, identificare l'ARN della definizione dell'attività. Apri la definizione dell'attività nella console Amazon ECS. Cerca la sezione dei volumi nella definizione dell'attività che definisce le mappature dei percorsi degli host.

Esamina la definizione dell'attività per determinare se l'accesso al file system host è necessario per la funzionalità del contenitore. Se non è richiesto l'accesso al file system host, create una nuova revisione della definizione del task e rimuovete tutte le definizioni di volume che utilizzano percorsi host. Se è richiesto l'accesso al file system host, prendete in considerazione la possibilità di configurare il contenitore per utilizzare un file system di sola lettura per evitare modifiche non autorizzate.

Il servizio Amazon ECS utilizza una definizione di attività configurata per condividere lo spazio dei nomi di processo di un host.

I contenitori Amazon ECS in esecuzione con namespace esposti possono potenzialmente accedere alle risorse del sistema host e ad altri namespace di container. Questa configurazione potrebbe consentire a un contenitore compromesso di superare il limite di isolamento, accedendo a processi, interfacce di rete o altre risorse al di fuori dell'ambito previsto.

Uno spazio dei nomi PID (Process ID) fornisce la separazione tra i processi. Impedisce la visibilità dei processi di sistema e consente il riutilizzo dei PID, incluso il PID 1. Se lo spazio dei nomi PID dell'host è condiviso con i contenitori, i contenitori possono visualizzare tutti i processi sul sistema host, riducendo l'isolamento a livello di processo. Ciò potrebbe comportare l'accesso non autorizzato ai processi host, inclusa la possibilità di manipolarli e terminarli. Seguendo i principi di sicurezza standard, mantenete il corretto isolamento dello spazio dei nomi per i contenitori.

Correzione: aggiorna le definizioni delle attività con namespace esposti

Apri la scheda Risorse dell'esposizione, identifica la definizione dell'attività con lo spazio dei nomi esposto. Apri la definizione dell'attività nella console Amazon ECS. Cerca le impostazioni PIDMode con il valore host, che condividerebbe i namespace degli ID del processo con l'host. Rimuovi le impostazioni di PidMode: host dalle definizioni delle attività per garantire che i contenitori funzionino con il corretto isolamento dello spazio dei nomi.

Il servizio Amazon ECS utilizza una definizione di attività configurata con credenziali in chiaro nelle variabili di ambiente.

I contenitori Amazon ECS con credenziali in chiaro nelle variabili di ambiente espongono informazioni di autenticazione sensibili che potrebbero essere compromesse se un utente malintenzionato accede alla definizione dell'attività, all'ambiente del contenitore o ai log del contenitore. Ciò crea un rischio significativo per la sicurezza, poiché le credenziali trapelate potrebbero essere utilizzate per accedere ad altri servizi o risorse. AWS

Correzione

Esegui una o più delle seguenti azioni per risolvere questa esposizione:

Sostituisci le credenziali in chiaro

Nel rilevamento dell'esposizione, identificate la definizione dell'attività con credenziali in chiaro. Apri la definizione dell'attività nella console Amazon ECS. Cerca le variabili di ambiente nella definizione del contenitore che contengono valori sensibili come chiavi di AWS accesso, password del database o token API.

Considerate le seguenti alternative per passare le credenziali:

- Invece di utilizzare le chiavi di AWS accesso, utilizza i ruoli di esecuzione delle attività e i ruoli di attività IAM per concedere le autorizzazioni ai contenitori.
- Memorizza le credenziali come segreti AWS Secrets Manager e fai riferimento ad esse nella definizione dell'attività.

Aggiornare le definizioni dell'attività

Crea una nuova revisione della definizione dell'attività che gestisca in modo sicuro le credenziali. Quindi aggiorna il tuo servizio Amazon ECS per utilizzare la nuova revisione della definizione delle attività.

Il servizio Amazon ECS ha un gruppo di sicurezza aperto

I gruppi di sicurezza fungono da firewall virtuali per le attività di Amazon ECS volte a controllare il traffico in entrata e in uscita. I gruppi di sicurezza aperti, che consentono l'accesso illimitato da qualsiasi indirizzo IP, possono esporre i contenitori ad accessi non autorizzati, aumentando il rischio di esposizione a strumenti di scansione automatizzati e attacchi mirati. Seguendo i principi di sicurezza standard, limita l'accesso dei gruppi di sicurezza a indirizzi IP e porte specifici.

Correzione

Esegui una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi le regole del gruppo di sicurezza e valuta la configurazione corrente

Apri la risorsa per Amazon ECS Security Group. Valuta quali porte sono aperte e accessibili da ampi intervalli di indirizzi IP, ad esempio`(0.0.0.0/0 or ::/0)`.

Modifica le regole del gruppo di sicurezza

Modifica le regole del gruppo di sicurezza per limitare l'accesso a intervalli o indirizzi IP affidabili specifici. Quando aggiorni le regole del gruppo di sicurezza, prendi in considerazione la possibilità di separare i requisiti di accesso per i diversi segmenti di rete creando regole per ogni intervallo IP di origine richiesto o limitando l'accesso a porte specifiche.

Modifica le regole dei gruppi di sicurezza

Considerate le seguenti opzioni per metodi di accesso alternativi:

- Session Manager fornisce un accesso sicuro alla shell alle istanze Amazon EC2 senza la necessità di porte in ingresso, gestione di chiavi SSH o manutenzione di host bastion.
- I NAC forniscono un ulteriore livello di sicurezza a livello di sottorete. A differenza dei gruppi di sicurezza, i NAC sono privi di stato e richiedono la definizione esplicita di regole in entrata e in uscita.

Il servizio Amazon ECS dispone di indirizzi IP pubblici

I servizi Amazon ECS con indirizzi IP pubblici assegnati alle loro attività sono accessibili direttamente da Internet. Sebbene ciò possa essere necessario per servizi che devono essere disponibili al pubblico, aumenta la superficie di attacco e il potenziale di accesso non autorizzato.

Correzione

Intraprendi una o più delle seguenti azioni per ovviare a questa esposizione:

Identifica i servizi con indirizzi IP pubblici

Nel rilevamento dell'esposizione, identifica il servizio Amazon ECS a cui sono assegnati indirizzi IP pubblici alle sue attività. Cerca l'`assignPublicIp`impostazione con il valore di `ENABLED` nella configurazione del servizio.

Aggiornare le definizioni dell'attività

Crea una nuova revisione della definizione dell'attività che disabiliti gli indirizzi IP pubblici. Quindi aggiorna il tuo servizio Amazon ECS per utilizzare la nuova revisione della definizione delle attività.

Implementa modelli di accesso alla rete privata

Per le istanze che eseguono applicazioni Web, prendi in considerazione l'utilizzo di un Load Balancer (LB). I LB possono essere configurati per consentire l'esecuzione delle istanze in sottoreti private mentre l'LB viene eseguito in una sottorete pubblica e gestisce il traffico Internet.

Il servizio Amazon ECS utilizza una definizione di attività configurata con la modalità di rete host abilitata.

I contenitori Amazon ECS in esecuzione con la modalità di rete host condividono lo spazio dei nomi di rete con l'host, consentendo l'accesso diretto alle interfacce di rete, alle porte e alle tabelle di routing dell'host. Questa configurazione aggira l'isolamento di rete fornito dai container, esponendo potenzialmente i servizi in esecuzione sul contenitore direttamente alle reti esterne e consentendo ai contenitori di modificare le impostazioni della rete host. Seguendo i principi di sicurezza standard, mantieni un adeguato isolamento di rete per i contenitori.

Correzione

Esegui una o più delle seguenti azioni per risolvere questa esposizione:

Disattiva la modalità di rete host

Nel rilevamento dell'esposizione, identifica la definizione dell'attività con la modalità di rete host. Apri la definizione dell'attività nella console Amazon ECS. Cerca l'impostazione NetworkMode con il valore host nella definizione dell'attività.

Considerate le seguenti opzioni per disabilitare la modalità di rete host:

- La modalità `awsvpc` di rete offre il massimo livello di isolamento della rete assegnando a ciascuna attività la propria elastic network interface.
- La modalità `bridge` di rete fornisce l'isolamento e consente al contempo la mappatura delle porte per esporre specifiche porte container all'host.

Aggiornare le definizioni dell'attività

Crea una nuova revisione della definizione dell'attività con la configurazione della modalità di rete aggiornata. Quindi aggiorna il tuo servizio Amazon ECS per utilizzare la nuova revisione della definizione delle attività.

Caratteristiche di raggiungibilità per i servizi Amazon ECS

Ecco le caratteristiche di raggiungibilità per i servizi Amazon ECS e le procedure di correzione suggerite.

Il servizio Amazon ECS è raggiungibile tramite Internet

Un servizio Amazon ECS che esegue attività su una sottorete pubblica è accessibile direttamente da Internet. Ciò aumenta la superficie di attacco e il rischio di accesso non autorizzato. Seguendo i principi di sicurezza standard, esegui attività su sottoreti private e consenti solo l'accesso a Internet richiesto dal servizio.

Correzione

Esegui una o più delle seguenti azioni per risolvere questa esposizione:

Esegui attività su una sottorete privata

Per spostare le tue attività da una sottorete pubblica, aggiorna la configurazione di rete per il tipo di avvio:

- Per Fargate, specifica le sottoreti private nella configurazione di rete del tuo servizio Amazon ECS e imposta su. `assignPublicIp` `DISABLED` Amazon ECS ospita ogni attività su una sottorete privata e ne indirizza il traffico in uscita attraverso un gateway NAT associato alla sottorete.
- Per EC2, avvia le istanze di container che forniscono la capacità del cluster su sottoreti private. Le attività utilizzano la rete privata dell'host e indirizzano il traffico in uscita attraverso un gateway NAT.

Utilizza un gateway NAT per l'accesso in uscita

Per le attività su una sottorete privata che richiedono l'accesso a Internet in uscita, utilizza un gateway NAT. Puoi utilizzare un gateway NAT per consentire alle attività di avviare connessioni in uscita a Internet e impedire le connessioni in entrata da Internet. Per ulteriori informazioni, consulta Connetti le applicazioni Amazon ECS a Internet nella Amazon ECS Developer Guide.

Utilizza un sistema di bilanciamento del carico per l'accesso in entrata

Per i servizi che devono accettare il traffico Internet, esegui le tue attività su sottoreti private utilizzando un sistema di bilanciamento del carico che funziona su una sottorete pubblica. Per aggiungere protezione contro gli exploit e i bot web, associa AWS Web Application Firewall (WAF) al tuo sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Utilizzare il bilanciamento del carico per distribuire il traffico del servizio Amazon ECS nella Amazon ECS Developer Guide.

Caratteristiche di vulnerabilità per i servizi Amazon ECS

Di seguito sono riportati i tratti di vulnerabilità per Amazon ECS e le procedure di correzione suggerite.

Il servizio Amazon ECS dispone di un contenitore con vulnerabilità software sfruttabili in rete con un'elevata probabilità di sfruttamento

1. Comprendi l'esposizione

   I risultati delle vulnerabilità dei pacchetti identificano i pacchetti software presenti nell' AWS ambiente che sono esposti a vulnerabilità ed esposizioni comuni (CVE). Gli aggressori possono sfruttare queste vulnerabilità prive di patch per compromettere la riservatezza, l'integrità o la disponibilità dei dati o per accedere ad altri sistemi. Le immagini dei contenitori ECR possono contenere rilevazioni di vulnerabilità dei pacchetti.
2. Correggi l'esposizione
   a. Aggiorna la versione del pacchetto

      Esamina la rilevazione della vulnerabilità del pacchetto per l'immagine del tuo contenitore ECR. Aggiorna la versione del pacchetto come suggerito da Amazon Inspector. Per ulteriori informazioni, consulta Visualizzazione dei dettagli relativi ai risultati di Amazon Inspector nella Amazon Inspector User Guide. La sezione Remediation dei dettagli di ricerca nella console Amazon Inspector indica quali comandi è possibile eseguire per aggiornare il pacchetto.
   b. Aggiorna le immagini dei contenitori di base

      Ricostruisci e aggiorna regolarmente le immagini dei contenitori di base per mantenerli aggiornati. Quando ricostruite un'immagine, non includete componenti non necessari per ridurre la superficie di attacco. Per istruzioni sulla ricostruzione dell'immagine di un contenitore, consulta Ricostruire spesso le immagini.

Il servizio Amazon ECS dispone di un contenitore con vulnerabilità software

I pacchetti software installati sui contenitori Amazon ECS possono essere esposti a vulnerabilità ed esposizioni comuni (CVE). Le vulnerabilità a bassa priorità rappresentano punti deboli di sicurezza con gravità o sfruttabilità inferiori rispetto alle vulnerabilità ad alta priorità. Sebbene queste vulnerabilità rappresentino un rischio meno immediato, gli aggressori possono comunque sfruttare queste vulnerabilità prive di patch per compromettere la riservatezza, l'integrità o la disponibilità dei dati o per accedere ad altri sistemi.

Correzione

Esegui una o più delle seguenti azioni per risolvere questa esposizione:

Aggiorna le immagini dei contenitori interessati

Consultate la sezione Riferimenti nella scheda Vulnerabilità della caratteristica. La documentazione del fornitore può includere indicazioni specifiche sulla correzione.

Applica la riparazione appropriata seguendo queste linee guida generali:

- Aggiorna le immagini dei contenitori per utilizzare le versioni con patch dei pacchetti interessati.
- Aggiorna le dipendenze interessate nell'applicazione alle versioni sicure più recenti.

Dopo aver aggiornato l'immagine del contenitore, inseriscila nel registro dei contenitori e aggiorna la definizione dell'attività Amazon ECS per utilizzare la nuova immagine.

Considerazioni future

Per rafforzare ulteriormente il livello di sicurezza delle immagini dei container, prendi in considerazione l'idea di seguire le best practice di Amazon ECS per le attività e la sicurezza dei container. Amazon Inspector può essere configurato per eseguire automaticamente la scansione dei CVE nei contenitori. Amazon Inspector può anche essere integrato con Security Hub per le riparazioni automatiche. Prendi in considerazione l'implementazione di un programma di patch regolare utilizzando Systems Manager Maintenance Windows per ridurre al minimo le interruzioni dei container.

Il servizio Amazon ECS dispone di un contenitore con un End-Of-Life sistema operativo

Il contenitore Amazon ECS si basa su un sistema operativo fuori uso che non è più supportato o gestito dallo sviluppatore originale. Ciò espone il contenitore a vulnerabilità di sicurezza e potenziali attacchi. Quando i sistemi operativi raggiungono la fine del ciclo di vita, i fornitori in genere smettono di rilasciare nuovi avvisi di sicurezza. Gli avvisi di sicurezza esistenti possono anche essere rimossi dai feed dei fornitori. Di conseguenza, Amazon Inspector potrebbe potenzialmente smettere di generare risultati per CVE noti, creando ulteriori lacune nella copertura di sicurezza.

Consulta i sistemi operativi fuori produzione nella Amazon Inspector User Guide per informazioni sui sistemi operativi che hanno raggiunto la fine del ciclo di vita che possono essere rilevati da Amazon Inspector.

Correzione: aggiornamento a una versione del sistema operativo supportata

Aggiornamento a una versione supportata del sistema operativo. Nel risultato dell'esposizione, aprite la risorsa per accedere alla risorsa interessata. Prima di aggiornare la versione del sistema operativo nell'immagine del contenitore, consulta le versioni disponibili in Supported Operating Systems nella Amazon Inspector User Guide per un elenco delle versioni del sistema operativo attualmente

supportate. Dopo aver aggiornato l'immagine del contenitore, inseriscila nel registro dei contenitori e aggiorna la definizione dell'attività Amazon ECS per utilizzare la nuova immagine.

Il servizio Amazon ECS dispone di un contenitore con pacchetti software dannosi

I pacchetti dannosi sono componenti software che contengono codice dannoso progettato per compromettere la riservatezza, l'integrità e la disponibilità dei sistemi e dei dati. I pacchetti dannosi rappresentano una minaccia attiva e critica per le immagini dei container Amazon ECS, poiché gli aggressori possono eseguire codice dannoso automaticamente senza sfruttare una vulnerabilità. Seguendo le migliori pratiche di sicurezza, rimuovi i pacchetti dannosi per proteggere i contenitori da potenziali attacchi.

Correzione: rimuovi i pacchetti dannosi

Esamina i dettagli del pacchetto dannoso nella sezione Riferimenti della scheda Vulnerabilità della caratteristica per comprendere la minaccia. Rimuovi i pacchetti dannosi identificati dalle immagini del contenitore, quindi ricostruiscili. Per ulteriori informazioni, consulta ContainerDependency nel AWS Riferimento sull'API di Amazon ECS.

Dopo aver aggiornato l'immagine del contenitore, inseriscila nel registro dei contenitori e aggiorna la definizione dell'attività Amazon ECS per utilizzare la nuova immagine. Per ulteriori informazioni, consulta la sezione Aggiornamento di una definizione di attività Amazon ECS utilizzando la console nella AWS Amazon ECS Developer Guide.

Caratteristiche di impatto per i servizi Amazon ECS

I tratti di impatto descrivono il potenziale raggio di esplosione di un'esposizione. Security Hub analizza le autorizzazioni effettive del AWS Identity and Access Management principale associato al servizio Amazon ECS per determinare le risorse downstream che un utente malintenzionato potrebbe raggiungere in caso di compromissione del servizio, nonché la criticità aziendale di tali risorse. Ogni caratteristica di impatto identifica uno specifico modello di escalation dei privilegi. Per ridurre il raggio d'azione, esaminate i percorsi di autorizzazione descritti in ogni caratteristica e rimuovete eventuali privilegi non necessari.

Seguendo i principi di sicurezza standard, concedi il privilegio minimo fornendo solo le autorizzazioni necessarie per eseguire un'attività. Sostituisci politiche generali con politiche circoscritte che garantiscano solo le azioni e le risorse specifiche necessarie. Per identificare le autorizzazioni non utilizzate da rimuovere, utilizza IAM Access Analyzer per generare consigli basati sulla cronologia degli accessi. Per ulteriori informazioni, consulta Findings for external and inused access e Apply least-privilege permissions nella IAM User Guide.

Dispone del percorso di esecutore privilegiato con pieno controllo

Il principale associato può passare un ruolo e inserire codice in una risorsa di calcolo che dispone già di autorizzazioni elevate. Ciò consente al principale di ottenere il pieno controllo sull'esecutore ed eseguire qualsiasi azione consentita dal ruolo dell'esecutore.

Ha un percorso diretto di escalation delle politiche

Il principale associato può modificare direttamente le politiche IAM per concedersi autorizzazioni aggiuntive, aumentando i propri privilegi senza risorse intermedie.

Ha un percorso di dirottamento delle politiche di fiducia

Il principale associato può modificare la politica di fiducia di un ruolo IAM per consentirsi di assumere quel ruolo, ottenendo le autorizzazioni del ruolo.

Ha un percorso di ransomware per i dati

Il principale associato può crittografare o eliminare i dati in un modo che potrebbe essere utilizzato per il ransomware, ad esempio crittografando gli oggetti Amazon S3 con una AWS KMS chiave gestita dal cliente e quindi modificando la politica della chiave.

Ha un percorso di rimozione della restrizione

Il principale associato può rimuovere le restrizioni di sicurezza come i limiti di autorizzazione, le politiche di controllo dei servizi o le dichiarazioni di rifiuto delle politiche basate sulle risorse, ampliando le funzionalità che possono fare gli altri principali o la risorsa stessa.

Ha il percorso pass role create executor

Il principale associato può creare una nuova risorsa di calcolo (come una funzione Lambda o un'istanza Amazon EC2) e assegnarle un ruolo privilegiato, riciclando efficacemente le proprie autorizzazioni attraverso la nuova risorsa.

Ha un percorso di esecuzione esistente di Swap Role

Il principale associato può modificare il ruolo IAM associato a una risorsa di elaborazione esistente, sostituendolo con un ruolo più privilegiato per aumentare l'accesso.

Ha un percorso di escalation della catena di ruoli

Il principale associato può assumere una sequenza di ruoli, in cui ogni ruolo della catena dispone di autorizzazioni progressivamente più ampie, fino a raggiungere infine un ruolo altamente privilegiato.

Dispone di un percorso di esecuzione privilegiato per il codice di iniezione

Il principale associato può iniettare codice in una risorsa di elaborazione in esecuzione che dispone di autorizzazioni elevate, eseguendo operazioni arbitrarie nell'ambito del ruolo privilegiato di tale risorsa.

Ha disabilitato il percorso di audit trail

Il responsabile associato può disabilitare i servizi di registrazione o monitoraggio CloudTrail, ad esempio coprire efficacemente le tracce durante o dopo un'escalation.

Ha accesso al percorso dell'esecutore esistente

Il principale associato può richiamare o connettersi a una risorsa di elaborazione esistente e utilizzare il ruolo associato per eseguire azioni privilegiate.

Dispone di un percorso di coniazione delle credenziali

Il principale associato può creare nuove credenziali a lungo termine (come chiavi di accesso o profili di accesso) per altri principali, stabilendo percorsi di accesso persistenti che sopravvivono alla rotazione delle password o alle scadenze delle sessioni.

Dispone di un percorso di accesso ai dati di accesso ai dati

Il responsabile associato può creare una risorsa di servizio e assegnarle un ruolo con accesso a dati sensibili, ottenendo l'accesso indiretto a tali dati tramite la nuova risorsa.

Ha un percorso pass role task hijack

Il principale associato può passare un ruolo a un'attività pianificata o basata su eventi (come una funzione Lambda attivata da un evento), consentendogli di eseguire codice arbitrario con le autorizzazioni di quel ruolo.

Ha un percorso di accesso ai dati a hop singolo

Il principale associato può accedere direttamente alle risorse di dati sensibili (come i bucket Amazon S3 o le tabelle DynamoDB) tramite le autorizzazioni esistenti, senza bisogno di passaggi di escalation intermedi.

Ha un percorso di avanzamento delle capacità

Il principale associato dispone di un percorso di assegnazione dei privilegi che ne migliora le capacità complessive oltre a quanto suggerirebbe l'assegnazione diretta delle autorizzazioni. Questa è una classificazione generale per i percorsi che non corrispondono a uno schema più specifico.

Criticità aziendale

La criticità aziendale della risorsa principale, stabilita dalle regole di automazione o dall'inferenza del nome e dei tag.

Correzione delle esposizioni per i cluster Amazon EKS

AWS Security Hub può generare risultati sull'esposizione per i cluster Amazon Elastic Kubernetes Service (Amazon EKS).

Il cluster Amazon EKS coinvolto nella rilevazione dell'esposizione e le relative informazioni identificative sono elencati nella sezione Risorse dei dettagli dei risultati. Puoi recuperare questi dettagli sulle risorse sulla console Security Hub o a livello di codice con il GetFindingsV2 funzionamento dell'API Security Hub CSPM.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la risoluzione fornite in questo argomento potrebbero richiedere ulteriori consultazioni in altre risorse. AWS

Indice

- Caratteristiche di configurazione errata per i cluster Amazon EKS
  - Il cluster Amazon EKS consente l'accesso pubblico
  - Il cluster Amazon EKS utilizza una versione Kubernetes non supportata
  - Il cluster Amazon EKS utilizza segreti Kubernetes non crittografati
- Caratteristiche di vulnerabilità per i cluster Amazon EKS

- Il cluster Amazon EKS ha un contenitore con vulnerabilità software sfruttabili in rete con un'alta probabilità di sfruttamento
- Il cluster Amazon EKS ha un contenitore con vulnerabilità software
- Il cluster Amazon EKS ha un contenitore con un sistema operativo End-Of-Life
- Il cluster Amazon EKS ha un contenitore con pacchetti software dannosi
- Il cluster Amazon EKS contiene file dannosi

Caratteristiche di configurazione errata per i cluster Amazon EKS

Ecco le caratteristiche di configurazione errata per i cluster Amazon EKS e i passaggi di correzione suggeriti.

Il cluster Amazon EKS consente l'accesso pubblico

L'endpoint del cluster Amazon EKS è l'endpoint che utilizzi per comunicare con il server API Kubernetes del tuo cluster. Per impostazione predefinita, questo endpoint è pubblico su Internet. Gli endpoint pubblici aumentano la superficie di attacco e il rischio di accessi non autorizzati al server API Kubernetes, consentendo potenzialmente agli aggressori di accedere o modificare le risorse del cluster o accedere a dati sensibili. Seguendo le migliori pratiche di sicurezza, limita l'accesso all'endpoint del tuo cluster Amazon EKS solo agli intervalli IP necessari.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Modifica l'accesso agli endpoint

Nel rilevamento dell'esposizione, apri la risorsa. Questo apre il cluster Amazon EKS interessato. Puoi configurare il cluster per utilizzare l'accesso privato, l'accesso pubblico o entrambi.

Con l'accesso privato, le richieste API Kubernetes che hanno origine nel VPC del cluster utilizzano l'endpoint VPC privato. Con l'accesso pubblico, le richieste API Kubernetes che provengono dall'esterno del VPC del cluster utilizzano l'endpoint pubblico.

Modifica o rimuovi l'accesso pubblico al cluster

Per modificare l'accesso agli endpoint per un cluster esistente, consulta Modifying cluster endpoint access nella Amazon Elastic Kubernetes Service User Guide. Implementa regole più restrittive basate su intervalli IP o gruppi di sicurezza specifici. Se è necessario un accesso pubblico limitato, limita l'accesso a intervalli di blocchi CIDR specifici o utilizza elenchi di prefissi.

Il cluster Amazon EKS utilizza una versione Kubernetes non supportata

Amazon EKS supporta ogni versione di Kubernetes per un periodo di tempo limitato. L'esecuzione di cluster con versioni di Kubernetes non supportate può esporre l'ambiente a vulnerabilità di sicurezza, poiché le patch CVE non verranno più rilasciate per le versioni obsolete. Le versioni non supportate possono contenere vulnerabilità di sicurezza note che possono essere sfruttate dagli aggressori e non dispongono di funzionalità di sicurezza che potrebbero essere disponibili nelle versioni più recenti. Seguendo le best practice di sicurezza, mantieni aggiornata la tua versione di Kubernetes.

Correzione: aggiorna la versione di Kubernetes

Nel rilevamento dell'esposizione, apri la risorsa. Questo apre il cluster Amazon EKS interessato. Prima di aggiornare il cluster, consulta le versioni disponibili con supporto standard nella Amazon Elastic Kubernetes Service User Guide per un elenco delle versioni Kubernetes attualmente supportate.

Il cluster Amazon EKS utilizza segreti Kubernetes non crittografati

I segreti Kubernetes sono, per impostazione predefinita, archiviati non crittografati nel data store sottostante del server API (etcd). Chiunque abbia accesso alle API o a etcd può recuperare o modificare un segreto. Per evitare che ciò accada, è necessario crittografare i segreti di Kubernetes inattivi. Se i segreti di Kubernetes non sono crittografati, sono vulnerabili all'accesso non autorizzato se etcd è compromesso. Poiché i segreti spesso contengono informazioni sensibili come password e token API, la loro esposizione potrebbe portare ad accessi non autorizzati ad altre applicazioni e dati. Seguendo le migliori pratiche di sicurezza, crittografa tutte le informazioni sensibili archiviate nei segreti di Kubernetes.

Soluzione: crittografa i segreti di Kubernetes

Amazon EKS supporta la crittografia dei segreti di Kubernetes utilizzando chiavi KMS tramite crittografia a inviluppo. Per abilitare la crittografia dei segreti Kubernetes per il tuo cluster EKS, consulta Encrypt Kubernetes secret with KMS su cluster esistenti nella Amazon EKS User Guide.

Caratteristiche di vulnerabilità per i cluster Amazon EKS

Ecco le caratteristiche di vulnerabilità dei cluster Amazon EKS.

Il cluster Amazon EKS ha un contenitore con vulnerabilità software sfruttabili in rete con un'alta probabilità di sfruttamento

I pacchetti software installati sui cluster Amazon EKS possono essere esposti a vulnerabilità ed esposizioni comuni (CVE). I CVE critici comportano rischi di sicurezza significativi per il tuo

ambiente. AWS Gli utenti non autorizzati possono sfruttare queste vulnerabilità prive di patch per compromettere la riservatezza, l'integrità o la disponibilità dei dati o per accedere ad altri sistemi. Le vulnerabilità critiche con elevata probabilità di sfruttamento rappresentano minacce alla sicurezza immediate, poiché il codice di exploit potrebbe essere già disponibile al pubblico e utilizzato attivamente dagli aggressori o dagli strumenti di scansione automatici. Seguendo le best practice di sicurezza, correggi queste vulnerabilità per proteggere la tua istanza dagli attacchi.

Correzione: aggiorna le istanze interessate

Aggiorna le immagini dei contenitori alle versioni più recenti che includono correzioni di sicurezza per le vulnerabilità identificate. Ciò comporta in genere la ricostruzione delle immagini dei contenitori con immagini di base o dipendenze aggiornate, quindi la distribuzione delle nuove immagini nel cluster Amazon EKS.

Il cluster Amazon EKS ha un contenitore con vulnerabilità software

I pacchetti software installati sui cluster Amazon EKS possono essere esposti a vulnerabilità ed esposizioni comuni (CVE). I CVE non critici rappresentano punti deboli di sicurezza con gravità o sfruttabilità inferiori rispetto ai CVE critici. Sebbene queste vulnerabilità rappresentino un rischio meno immediato, gli aggressori possono comunque sfruttare queste vulnerabilità prive di patch per compromettere la riservatezza, l'integrità o la disponibilità dei dati o per accedere ad altri sistemi. Seguendo le best practice di sicurezza, correggi queste vulnerabilità per proteggere la tua istanza dagli attacchi.

Correzione: aggiorna le istanze interessate

Aggiorna le immagini dei contenitori alle versioni più recenti che includono correzioni di sicurezza per le vulnerabilità identificate. Ciò comporta in genere la ricostruzione delle immagini dei contenitori con immagini di base o dipendenze aggiornate, quindi la distribuzione delle nuove immagini nel cluster Amazon EKS.

Il cluster Amazon EKS ha un contenitore con un sistema operativo End-Of-Life

L'immagine del contenitore Amazon EKS si basa su un sistema operativo fuori uso che non è più supportato o gestito dallo sviluppatore originale. Ciò espone il contenitore a vulnerabilità di sicurezza e potenziali attacchi. Quando i sistemi operativi raggiungono la fine del ciclo di vita, i fornitori in genere smettono di rilasciare nuovi avvisi di sicurezza. Gli avvisi di sicurezza esistenti possono anche essere rimossi dai feed dei fornitori. Di conseguenza, Amazon Inspector potrebbe potenzialmente interrompere la generazione di risultati per CVE noti, creando ulteriori lacune nella copertura di sicurezza.

Consulta i sistemi operativi fuori produzione nella Guida per l'utente di Amazon Inspector per informazioni sui sistemi operativi che hanno raggiunto la fine del loro ciclo di vita e che possono essere rilevati da Amazon Inspector.

Soluzione: aggiornamento a una versione del sistema operativo supportata

Aggiornamento a una versione supportata del sistema operativo. Nella rilevazione dell'esposizione, apri la risorsa per accedere alla risorsa interessata. Prima di aggiornare la versione del sistema operativo nell'immagine del contenitore, consulta le versioni disponibili in Supported Operating Systems nella Amazon Inspector User Guide per un elenco delle versioni del sistema operativo attualmente supportate. Dopo aver aggiornato l'immagine del contenitore, ricostruisci e ridistribuisci i contenitori nel cluster Amazon EKS.

Il cluster Amazon EKS ha un contenitore con pacchetti software dannosi

I pacchetti dannosi sono componenti software che contengono codice dannoso progettato per compromettere la riservatezza, l'integrità e la disponibilità dei tuoi sistemi e dati. I pacchetti dannosi rappresentano una minaccia attiva e critica per il tuo cluster Amazon EKS, poiché gli aggressori possono eseguire codice dannoso automaticamente senza sfruttare una vulnerabilità. Seguendo le migliori pratiche di sicurezza, rimuovi i pacchetti dannosi per proteggere il cluster da potenziali attacchi.

Correzione: rimuovi i pacchetti dannosi

Esamina i dettagli dei pacchetti dannosi nella sezione Riferimenti della scheda Vulnerabilità della caratteristica per comprendere la minaccia. Rimuovi i pacchetti dannosi identificati dalle immagini dei contenitori. Quindi, elimina i contenitori con l'immagine compromessa.

Aggiorna le tue distribuzioni Kubernetes per utilizzare le immagini dei contenitori aggiornate. Quindi, implementa le modifiche e ridistribuisci i tuoi pod.

Il cluster Amazon EKS contiene file dannosi

I file dannosi contengono codice dannoso progettato per compromettere la riservatezza, l'integrità e la disponibilità dei tuoi sistemi e dati. I file dannosi rappresentano una minaccia attiva e critica per il cluster, poiché gli aggressori possono eseguire codice dannoso automaticamente senza sfruttare una vulnerabilità. Seguendo le best practice di sicurezza, rimuovi i file dannosi per proteggere il cluster da potenziali attacchi.

Correzione: rimuovi i file dannosi

Per identificare lo specifico volume di Amazon Elastic Block Store (Amazon EBS) che contiene file dannosi, consulta la sezione Risorse con i dettagli relativi alla caratteristica. Dopo aver identificato il volume con il file dannoso, rimuovi i file dannosi identificati. Dopo aver rimosso i file dannosi, valuta la possibilità di eseguire una scansione per verificare che tutti i file che potrebbero essere stati installati dal file dannoso siano stati rimossi. Per ulteriori informazioni, consulta Avvio della scansione On-demand antimalware GuardDuty in.

Correzione delle esposizioni per gli utenti IAM

AWS Security Hub può generare risultati di esposizione per gli utenti AWS Identity and Access Management (IAM).

Nella console Security Hub, l'utente IAM coinvolto in un rilevamento dell'esposizione e le relative informazioni identificative sono elencati nella sezione Risorse dei dettagli del risultato. A livello di codice, è possibile recuperare i dettagli delle risorse con il GetFindingsV2funzionamento dell'API CSPM Security Hub.

Dopo aver identificato la risorsa coinvolta in un rilevamento dell'esposizione, puoi eliminare la risorsa se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per mitigare il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato sull'esposizione contiene i problemi identificati in diversi argomenti relativi alla correzione. Al contrario, è possibile risolvere un problema di esposizione e ridurne il livello di gravità affrontando un solo argomento di correzione. L'approccio alla risoluzione dei rischi dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida sulla correzione fornite in questo argomento potrebbero richiedere ulteriori consultazioni in altre risorse. AWS

Le migliori pratiche IAM consigliano di creare ruoli IAM o di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee invece di creare singoli utenti IAM. Se questa è un'opzione per la tua organizzazione e il tuo caso d'uso, passa ai ruoli o alla federazione invece di utilizzare gli utenti IAM. Per ulteriori informazioni, consulta Utenti IAM nella Guida per l'utente di IAM.

Indice

- Caratteristiche di configurazione errate per gli utenti IAM
  - L'utente IAM non ha l'MFA abilitata
  - Il AWS l'account per l'utente IAM ha politiche di password deboli
  - L'utente IAM dispone di chiavi di accesso non ruotate
  - L'utente IAM dispone di una policy che consente l'accesso illimitato alla decrittografia delle chiavi KMS
- Caratteristiche di accesso non utilizzate per gli utenti IAM
- Caratteristiche di impatto per gli utenti IAM
  - Dispone di un percorso di esecutore privilegiato con pieno controllo
  - Ha un percorso diretto di escalation delle politiche
  - Dispone di un percorso di dirottamento delle politiche di fiducia
  - Ha un percorso di ransomware per i dati
  - Ha un percorso di rimozione della restrizione
  - Ha un percorso di creazione esecutore del ruolo
  - Ha un percorso di esecuzione esistente di Swap Role
  - Ha un percorso di escalation della catena di ruoli
  - Dispone di un percorso di esecutore privilegiato per il codice di iniezione
  - Ha disabilitato il percorso di audit trail
  - Ha accesso al percorso dell'esecutore esistente
  - Dispone di un percorso di coniazione delle credenziali
  - Dispone di un percorso di accesso ai dati di accesso ai dati
  - Ha un percorso di dirottamento del ruolo
  - Dispone di un percorso di accesso ai dati a hop singolo
  - Ha un percorso di avanzamento delle capacità
  - Criticità aziendale

Caratteristiche di configurazione errate per gli utenti IAM

Ecco le caratteristiche di configurazione errata per gli utenti IAM e le procedure di correzione suggerite.

L'utente IAM non ha l'MFA abilitata

Multi-factor l'autenticazione (MFA) aggiunge un ulteriore livello di protezione oltre a nome utente e password. Quando l'MFA è abilitata e un utente IAM accede a un AWS sito Web, gli viene richiesto il nome utente, la password e un codice di autenticazione dal dispositivo AWS MFA. L'entità principal di autenticazione deve possedere un dispositivo che genera una chiave legata al fattore tempo e deve essere a conoscenza delle credenziali. Senza MFA, se la password di un utente viene compromessa, un utente malintenzionato ottiene l'accesso completo alle autorizzazioni dell'utente. AWS Seguendo i principi di sicurezza standard, abilita l'MFA per tutti gli account e gli utenti che hanno Console di gestione AWS accesso.

Correzione

Esegui una o più delle seguenti azioni per ovviare a questa esposizione:

Esamina i tipi di MFA

AWS supporta i seguenti tipi di MFA:

- Passkey e chiavi di sicurezza
- Applicazioni di autenticazione virtuale
- Token TOTP hardware

Sebbene l'autenticazione con un dispositivo fisico offra in genere una protezione di sicurezza più rigorosa, l'utilizzo di qualsiasi tipo di MFA è più sicuro rispetto alla disattivazione dell'MFA.

Abilitare MFA

Per abilitare il tipo di MFA più adatto alle tue esigenze, consulta l'AWS autenticazione a più fattori in IAM nella IAM User Guide. Segui i passaggi per il tipo di MFA specifico che desideri implementare. Per le organizzazioni che gestiscono molti utenti, potresti voler imporre l'utilizzo della MFA richiedendo l'accesso a risorse sensibili.

Il AWS l'account per l'utente IAM ha politiche di password deboli

Le policy relative alle password aiutano a proteggere dagli accessi non autorizzati imponendo requisiti minimi di complessità per le password degli utenti IAM. Senza politiche solide in materia di password, aumenta il rischio che gli account utente possano essere compromessi mediante l'indovinazione delle password o attacchi di forza bruta. Seguendo i principi di sicurezza standard,

implementa una politica di password sicura per garantire che gli utenti creino password complesse e difficili da indovinare.

Correzione

Esegui una o più delle seguenti azioni per ovviare a questa esposizione:

Configura una politica di password sicura

Vai alla dashboard IAM e vai alle impostazioni dell'account. Controlla le attuali impostazioni delle politiche relative alle password per il tuo account, tra cui la lunghezza minima, i tipi di caratteri richiesti e le impostazioni di scadenza della password.

Per impostare la politica in materia di password, segui almeno queste best practice:

- Richiede almeno un carattere maiuscolo.
- Richiede almeno un carattere minuscolo.
- Richiede almeno un simbolo.
- Richiede almeno un numero.
- Richiede almeno otto caratteri.

Ulteriori considerazioni sulla sicurezza

Prendi in considerazione queste misure di sicurezza aggiuntive oltre a una solida politica in materia di password:

- L'MFA aggiunge un ulteriore livello di sicurezza richiedendo una forma di autenticazione aggiuntiva. Questo aiuta a prevenire l'accesso non autorizzato anche se le credenziali sono compromesse.
- Impostazione di elementi condizionali per limitare quando e come le autorizzazioni amministrative possono essere utilizzate in base a fattori come l'IP di origine o l'età dell'MFA.

L'utente IAM dispone di chiavi di accesso non ruotate

Le chiavi di accesso sono costituite da un ID della chiave di accesso e da una chiave di accesso segreta che consentono l'accesso programmatico alle risorse. AWS Quando le chiavi di accesso rimangono invariate per lunghi periodi di tempo, aumentano il rischio di accesso non autorizzato in caso di compromissione. Seguendo le migliori pratiche di sicurezza, ruota le chiavi di accesso ogni

90 giorni per ridurre al minimo la finestra di opportunità per gli aggressori di utilizzare credenziali compromesse.

Correzione: ruotare le chiavi di accesso

Nel rilevamento dell'esposizione, apri la risorsa. Si apre la finestra dei dettagli dell'utente. Per ruotare le chiavi di accesso, consulta Manage access keys for IAM users nella IAM User Guide.

L'utente IAM dispone di una policy che consente l'accesso illimitato alla decrittografia delle chiavi KMS

AWS KMS ti consente di creare e gestire chiavi crittografiche utilizzate per proteggere i tuoi dati. Le policy IAM che consentono autorizzazioni di AWS KMS decrittografia illimitate (ad esempio, `kms:Decrypt` o`kms:ReEncryptFrom`) su tutte le chiavi KMS possono portare all'accesso non autorizzato ai dati se le credenziali di un utente IAM vengono compromesse. Se un utente malintenzionato ottiene l'accesso a queste credenziali, potrebbe potenzialmente decrittografare tutti i dati crittografati presenti nell'ambiente dell'utente, inclusi i dati sensibili. Seguendo le migliori pratiche di sicurezza, implementate il privilegio minimo limitando le autorizzazioni di AWS KMS decrittografia solo alle chiavi specifiche di cui gli utenti hanno bisogno per le loro funzioni lavorative.

Correzione

Intraprendi una o più delle seguenti azioni per ovviare a questa esposizione:

Implementazione dell'accesso con privilegi minimi

Nel rilevamento dell'esposizione, apri la risorsa. Si apre la finestra IAM Policy. Cerca le autorizzazioni in KMS che consentano KMS:Decrypt o `kms:ReEncryptFrom` con una specifica di risorsa di. `KMS:*` `"*"`

Aggiorna la politica per limitare le autorizzazioni di AWS KMS decrittografia solo alle chiavi specifiche necessarie. Modifica la politica per sostituire la `"*"` risorsa con gli ARN specifici delle chiavi richieste. AWS KMS

Considerazioni sulla configurazione sicura

Valuta la possibilità di aggiungere condizioni per limitare ulteriormente l'utilizzo di queste autorizzazioni. Ad esempio, puoi limitare le operazioni di decrittografia a specifici endpoint VPC o intervalli IP di origine. Puoi anche configurare le politiche chiave per limitare ulteriormente chi può utilizzare chiavi KMS specifiche.

Caratteristiche di accesso non utilizzate per gli utenti IAM

Quando un utente IAM ha autorizzazioni, chiavi di accesso o password non utilizzate, Security Hub può includerle come caratteristiche contestuali nei risultati di esposizione per quell'utente. Queste caratteristiche sono generate da IAM Access Analyzer gestito dal servizio e forniscono un contesto aggiuntivo sulla posizione di sicurezza dell'utente. Le caratteristiche di accesso non utilizzate non sono la causa principale del rilevamento dell'esposizione, ma indicano che l'utente dispone di più autorizzazioni del necessario, il che aumenta il potenziale impatto in caso di compromissione delle credenziali dell'utente.

In particolare, per le autorizzazioni non utilizzate, è possibile generare una raccomandazione sulla politica dei privilegi minimi che mostri una politica sostitutiva limitata. Per ulteriori informazioni, consulta the section called "Raccomandazioni politiche".

Caratteristiche di impatto per gli utenti IAM

I tratti di impatto descrivono il potenziale raggio di esplosione di un'esposizione. Security Hub analizza le autorizzazioni effettive del AWS Identity and Access Management principale associato all'utente IAM per determinare le risorse a valle che un aggressore potrebbe raggiungere se l'utente IAM viene compromesso, nonché la criticità aziendale di tali risorse. Ogni caratteristica di impatto identifica uno specifico modello di escalation dei privilegi. Per ridurre il raggio d'azione, esaminate i percorsi di autorizzazione descritti in ogni caratteristica e rimuovete eventuali privilegi non necessari.

Seguendo i principi di sicurezza standard, concedi il privilegio minimo fornendo solo le autorizzazioni necessarie per eseguire un'attività. Sostituisci politiche generali con politiche circoscritte che garantiscano solo le azioni e le risorse specifiche necessarie. Per identificare le autorizzazioni non utilizzate da rimuovere, utilizza IAM Access Analyzer per generare consigli basati sulla cronologia degli accessi. Per ulteriori informazioni, consulta Findings for external and inused access e Apply least-privilege permissions nella IAM User Guide.

Dispone di un percorso di esecutore privilegiato con pieno controllo

Il principale associato può passare un ruolo e inserire codice in una risorsa di calcolo che dispone già di autorizzazioni elevate. Ciò consente al principale di ottenere il pieno controllo sull'esecutore ed eseguire qualsiasi azione consentita dal ruolo dell'esecutore.

Ha un percorso diretto di escalation delle politiche

Il principale associato può modificare direttamente le politiche IAM per concedersi autorizzazioni aggiuntive, aumentando i propri privilegi senza risorse intermedie.

Dispone di un percorso di dirottamento delle politiche di fiducia

Il principale associato può modificare la politica di fiducia di un ruolo IAM per consentirsi di assumere quel ruolo, ottenendo le autorizzazioni del ruolo.

Ha un percorso di ransomware per i dati

Il principale associato può crittografare o eliminare i dati in un modo che potrebbe essere utilizzato per il ransomware, ad esempio crittografando gli oggetti Amazon S3 con una AWS KMS chiave gestita dal cliente e quindi modificando la politica della chiave.

Ha un percorso di rimozione della restrizione

Il principale associato può rimuovere le restrizioni di sicurezza come i limiti di autorizzazione, le politiche di controllo dei servizi o le dichiarazioni di rifiuto delle politiche basate sulle risorse, ampliando le funzionalità che possono fare gli altri principali o la risorsa stessa.

Ha un percorso di creazione esecutore del ruolo

Il principale associato può creare una nuova risorsa di calcolo (come una funzione Lambda o un'istanza Amazon EC2) e assegnarle un ruolo privilegiato, riciclando efficacemente le proprie autorizzazioni attraverso la nuova risorsa.

Ha un percorso di esecuzione esistente di Swap Role

Il principale associato può modificare il ruolo IAM associato a una risorsa di elaborazione esistente, sostituendolo con un ruolo più privilegiato per aumentare l'accesso.

Ha un percorso di escalation della catena di ruoli

Il principale associato può assumere una sequenza di ruoli, in cui ogni ruolo della catena dispone di autorizzazioni progressivamente più ampie, fino a raggiungere infine un ruolo altamente privilegiato.

Dispone di un percorso di esecutore privilegiato per il codice di iniezione

Il principale associato può iniettare codice in una risorsa di elaborazione in esecuzione che dispone di autorizzazioni elevate, eseguendo operazioni arbitrarie nell'ambito del ruolo privilegiato di tale risorsa.

Ha disabilitato il percorso di audit trail

Il responsabile associato può disabilitare i servizi di registrazione o monitoraggio CloudTrail, ad esempio coprire efficacemente le proprie tracce durante o dopo un'escalation.

Ha accesso al percorso dell'esecutore esistente

Il principale associato può richiamare o connettersi a una risorsa di elaborazione esistente e utilizzare il ruolo associato per eseguire azioni privilegiate.

Dispone di un percorso di coniazione delle credenziali

Il principale associato può creare nuove credenziali a lungo termine (come chiavi di accesso o profili di accesso) per altri principali, stabilendo percorsi di accesso persistenti che sopravvivono alla rotazione delle password o alle scadenze delle sessioni.

Dispone di un percorso di accesso ai dati di accesso ai dati

Il responsabile associato può creare una risorsa di servizio e assegnarle un ruolo con accesso a dati sensibili, ottenendo l'accesso indiretto a tali dati tramite la nuova risorsa.

Ha un percorso di dirottamento del ruolo

Il principale associato può passare un ruolo a un'attività pianificata o basata su eventi (come una funzione Lambda attivata da un evento), consentendogli di eseguire codice arbitrario con le autorizzazioni di quel ruolo.

Dispone di un percorso di accesso ai dati a hop singolo

Il principale associato può accedere direttamente alle risorse di dati sensibili (come i bucket Amazon S3 o le tabelle DynamoDB) tramite le autorizzazioni esistenti, senza bisogno di passaggi di escalation intermedi.

Ha un percorso di avanzamento delle capacità

Il principale associato dispone di un percorso di assegnazione dei privilegi che ne migliora le capacità complessive oltre a quanto suggerirebbe l'assegnazione diretta delle autorizzazioni. Questa è una classificazione generale per i percorsi che non corrispondono a uno schema più specifico.

Criticità aziendale

La criticità aziendale della risorsa principale, stabilita dalle regole di automazione o dall'inferenza del nome e dei tag.

Riparazione delle esposizioni per AWS Lambda funzioni

AWS Security Hub può generare risultati di esposizione per AWS Lambda le funzioni.

Sulla console Security Hub, la funzione Lambda coinvolta in un rilevamento dell'esposizione e le relative informazioni di identificazione sono elencate nella sezione Risorse dei dettagli del risultato. A livello di codice, è possibile recuperare i dettagli delle risorse con il GetFindingsV2funzionamento dell'API CSPM Security Hub.

Dopo aver identificato la risorsa coinvolta in un rilevamento dell'esposizione, puoi eliminare la risorsa se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per mitigare il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato sull'esposizione contiene i problemi identificati in diversi argomenti relativi alla correzione. Al contrario, è possibile risolvere un problema di esposizione e ridurne il livello di gravità affrontando un solo argomento di correzione. L'approccio alla risoluzione dei rischi dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida sulla correzione fornite in questo argomento potrebbero richiedere ulteriori consultazioni in altre risorse. AWS

Indice

- Caratteristiche di configurazione errate per le funzioni Lambda
  - La funzione Lambda viene implementata all'esterno di un Amazon VPC
  - La funzione Lambda è accessibile tramite API Gateway senza autorizzazione
  - La funzione Lambda è esposta tramite un AgentCore gateway Amazon Bedrock senza alcun autorizzatore configurato
  - La funzione Lambda è esposta tramite un AgentCore gateway Amazon Bedrock che consente l'accesso pubblico non autenticato
- Caratteristiche di raggiungibilità per le funzioni Lambda
  - La funzione Lambda può essere invocata pubblicamente
- Caratteristiche di vulnerabilità per le funzioni Lambda
  - La funzione Lambda presenta vulnerabilità software sfruttabili dalla rete
  - La funzione Lambda presenta vulnerabilità software
  - La funzione Lambda contiene pacchetti software dannosi
  - La funzione Lambda presenta vulnerabilità nel codice

- Caratteristiche di impatto per le funzioni Lambda
  - Dispone di un percorso di esecutore privilegiato con pieno controllo
  - Ha un percorso diretto di escalation delle politiche
  - Ha un percorso di dirottamento delle politiche di fiducia
  - Ha un percorso di ransomware per i dati
  - Ha un percorso di rimozione della restrizione
  - Ha il percorso pass role create executor
  - Ha un percorso di esecuzione esistente di Swap Role
  - Ha un percorso di escalation della catena di ruoli
  - Dispone di un percorso di esecutore privilegiato per il codice di iniezione
  - Ha disabilitato il percorso di audit trail
  - Ha accesso al percorso dell'esecutore esistente
  - Dispone di un percorso di coniazione delle credenziali
  - Dispone di un percorso di accesso ai dati di tipo pass role
  - Ha un percorso di dirottamento del ruolo
  - Ha un percorso di accesso ai dati a hop singolo
  - Ha un percorso di avanzamento delle capacità
  - Criticità aziendale

Caratteristiche di configurazione errate per le funzioni Lambda

Di seguito sono riportate le caratteristiche di errata configurazione delle funzioni Lambda e i passaggi di correzione suggeriti.

La funzione Lambda viene implementata all'esterno di un Amazon VPC

Per impostazione predefinita, le funzioni Lambda vengono distribuite con accesso alla rete Internet pubblica. Questa configurazione predefinita offre alle funzioni Lambda la possibilità di raggiungere gli endpoint di AWS servizio e le API esterne, ma le espone anche a potenziali rischi per la sicurezza. Le funzioni con accesso a Internet potrebbero essere utilizzate per esfiltrare dati, comunicare con server non autorizzati o diventare punti di accesso per attori esterni se compromesse. Amazon VPC fornisce l'isolamento della rete limitando le funzioni Lambda a comunicare solo con risorse all'interno della rete privata definita. Seguendo i principi di sicurezza standard, implementa le funzioni Lambda all'interno di un VPC per migliorare la sicurezza attraverso l'isolamento della rete.

Riparazione: collega la funzione al VPC

Nella ricerca sull'esposizione, scegli il link alla risorsa. Si apre la funzione Lambda nella console Lambda. Per proteggere la tua funzione Lambda limitandone l'accesso alla rete, collegala a un VPC dotato dei controlli di rete appropriati.

Prima di collegare la tua funzione a un VPC, pianifica l'accesso al servizio di cui potrebbe aver bisogno, poiché le funzioni nelle sottoreti private AWS senza gateway NAT o endpoint VPC non possono raggiungere le API di servizio. AWS Per informazioni su come collegare una funzione Lambda a un Amazon VPC nel tuo account, consulta Allegare le funzioni Lambda a un Amazon VPC nel tuo. Account AWS Prendi in considerazione l'utilizzo di endpoint VPC per la connettività dei servizi senza accesso a Internet se la tua funzione richiede l'accesso ai AWS servizi da una sottorete privata. Configura un gateway NAT se hai bisogno di connettività Internet in uscita da sottoreti private.

La funzione Lambda è accessibile tramite API Gateway senza autorizzazione

I metodi API Gateway senza autorizzazione consentono a qualsiasi chiamante con accesso all'API Gateway di richiamare la funzione Lambda integrata senza verifica dell'identità. Questa configurazione crea rischi per la sicurezza, in quanto i chiamanti possono richiamare la funzione Lambda senza un'autorizzazione adeguata, con il rischio di abuso delle funzionalità della funzione, consumo di risorse, accesso a dati sensibili o operazioni non autorizzate. Sebbene API Gateway possa avere controlli di accesso a livello di rete, la mancanza di autorizzazione a livello di metodo potrebbe consentire la chiamata gratuita della funzione da parte di qualsiasi chiamante con accesso di rete all'API Gateway. Seguendo le best practice di sicurezza, implementa meccanismi di autorizzazione appropriati per i metodi API Gateway che si integrano con le funzioni Lambda.

Correzione: configurazione dell'autenticazione API Gateway

Nella scheda Risorse dell'esposizione, scegli il link della risorsa per accedere al metodo API Gateway. Rivedi la configurazione di autorizzazione corrente e implementa i meccanismi di autenticazione appropriati.

API Gateway supporta diverse opzioni di autenticazione tra cui AWS IAM, pool di utenti di Amazon Cognito, autorizzatori Lambda e chiavi API. Scegli il metodo di autenticazione più adatto ai tuoi requisiti di sicurezza e al tuo caso d'uso. Per istruzioni dettagliate sulla configurazione dell'autenticazione, consulta Controllare e gestire l'accesso a un'API REST in API Gateway nella API Gateway Developer Guide.

La funzione Lambda è esposta tramite un AgentCore gateway Amazon Bedrock senza alcun autorizzatore configurato

I AgentCore gateway Amazon Bedrock espongono le funzioni Lambda come strumenti che gli agenti AI possono scoprire e richiamare. Un gateway senza autorizzazione accetta le richieste senza verificare l'identità del chiamante. Qualsiasi chiamante che ottiene l'endpoint del gateway può elencare gli strumenti esposti dal gateway e richiamare la funzione Lambda integrata senza autenticazione. Ciò crea rischi per la sicurezza, poiché le chiamate non autenticate potrebbero portare all'abuso delle funzionalità delle funzioni, all'accesso a dati sensibili o a operazioni non autorizzate nell'ambiente. Seguendo le best practice di sicurezza, configura l'autorizzazione in entrata sui AgentCore gateway Amazon Bedrock che fronteggiano le funzioni Lambda.

Correzione: configura l'autorizzazione in entrata del gateway

Nella sezione Risorse del risultato sull'esposizione, annota l'identificatore del gateway. Apri la AgentCore console Amazon Bedrock, scegli il gateway e rivedi la sua configurazione di autorizzazione in entrata.

I AgentCore gateway Amazon Bedrock supportano l'autorizzazione in entrata con un autorizzatore JSON Web Token (JWT) tramite un provider di identità OAuth-compliant come Amazon Cognito. Configura un autorizzatore in modo che il gateway convalidi il token del chiamante prima di soddisfare le richieste degli strumenti. Per istruzioni dettagliate, consulta la sezione Prerequisiti per l'utilizzo del servizio AgentCore gateway Amazon Bedrock nella Amazon Bedrock AgentCore Developer Guide.

La funzione Lambda è esposta tramite un AgentCore gateway Amazon Bedrock che consente l'accesso pubblico non autenticato

I AgentCore gateway Amazon Bedrock possono adottare una policy basata sulle risorse che controlla quali principali possono richiamare il gateway. Una politica di gateway che include «*» come principale consente a qualsiasi chiamante di richiamare gli strumenti esposti dal gateway, inclusa la funzione Lambda integrata. Questa configurazione aggira i controlli di accesso basati sull'identità e crea rischi significativi perché i chiamanti non autenticati possono richiamare la funzione. Ciò potrebbe portare all'abuso delle funzionalità funzionali, all'accesso a dati sensibili o a operazioni non autorizzate. Seguendo le migliori pratiche di sicurezza, limita l'accesso al gateway solo ai principali autorizzati.

Correzione: limita la politica basata sulle risorse del gateway

Apri il gateway identificato nella sezione Risorse del sondaggio sull'esposizione e rivedi la sua politica basata sulle risorse. Rimuovi le dichiarazioni che consentono «*» come principale. Concedi l'accesso solo agli ID di AWS account o ai principali IAM specifici che devono richiamare il gateway.

Per ulteriori informazioni sulla limitazione dell'accesso ai AgentCore gateway Amazon Bedrock, consulta il controllo degli Fine-grained accessi per Amazon Bedrock Gateway AgentCore nella Amazon Bedrock Developer Guide. AgentCore

Caratteristiche di raggiungibilità per le funzioni Lambda

Di seguito sono riportati i tratti di raggiungibilità per le funzioni Lambda e i passaggi di correzione suggeriti.

La funzione Lambda può essere invocata pubblicamente

Le policy basate sulle risorse di Lambda determinano chi può richiamare le tue funzioni. Una funzione con una politica delle risorse che include «*» come principale (o nessuna) consente a qualsiasi utente autenticato AWS di richiamarla. Ciò comporta un rischio significativo, in particolare per le funzioni che elaborano dati sensibili, modificano risorse o dispongono di autorizzazioni elevate. Gli utenti non autorizzati potrebbero sfruttare questa configurazione per eseguire operazioni indesiderate, esponendo potenzialmente dati, manipolando risorse o abusando delle funzionalità. Seguendo le best practice di sicurezza, limita l'accesso alla funzione Lambda solo ai principali autorizzati.

Correzione: modifica la politica basata sulle risorse della funzione

Nella scheda Risorse dell'esposizione, apri la risorsa con il collegamento ipertestuale. Si apre la funzione Lambda nella console Lambda. Limita l'accesso alla tua funzione Lambda specificando solo gli ID di AWS account autorizzati o i principali IAM specifici (utenti, ruoli o servizi) nella policy basata sulle risorse. È possibile modificare le politiche basate sulle risorse solo a livello di codice.

Caratteristiche di vulnerabilità per le funzioni Lambda

Di seguito sono riportati i tratti di vulnerabilità per le funzioni Lambda e le procedure di correzione suggerite.

La funzione Lambda presenta vulnerabilità software sfruttabili dalla rete

I pacchetti software utilizzati nel codice della funzione Lambda possono contenere vulnerabilità ed esposizioni comuni (CVE) che hanno un'alta probabilità di essere sfruttate. I CVE critici rappresentano rischi significativi per la sicurezza dell'ambiente. AWS Gli aggressori possono sfruttare queste vulnerabilità prive di patch per compromettere la riservatezza, l'integrità o la disponibilità dei dati o per accedere ad altri sistemi. Le vulnerabilità critiche con un'elevata probabilità di sfruttamento

rappresentano minacce immediate alla sicurezza, poiché il codice di exploit potrebbe già essere disponibile al pubblico e utilizzato attivamente dagli aggressori o dagli strumenti di scansione automatizzati. Seguendo le migliori pratiche di sicurezza, correggi queste vulnerabilità per proteggere la tua funzione dagli attacchi.

Correzione: aggiorna le funzioni interessate

Consultate la sezione Riferimenti nella scheda Vulnerabilità per conoscere la caratteristica. La documentazione del fornitore potrebbe includere linee guida specifiche per la correzione. Aggiorna le librerie vulnerabili alle versioni sicure più recenti seguendo le procedure consigliate dal fornitore.

In genere, il flusso di lavoro di riparazione dipende dal fatto che il pacchetto Lambda sia stato distribuito caricando un file zip o creando una funzione Lambda con un'immagine del contenitore. Dopo aver aggiornato le librerie, aggiorna il codice della funzione Lambda per utilizzare la versione fissa. Successivamente, distribuisci la versione aggiornata.

La funzione Lambda presenta vulnerabilità software

Le funzioni Lambda utilizzano spesso librerie e dipendenze di terze parti che possono contenere vulnerabilità di sicurezza con gravità o sfruttabilità inferiori rispetto ai CVE critici. Sebbene queste vulnerabilità non critiche possano non essere sfruttabili immediatamente, rappresentano comunque punti deboli di sicurezza che potrebbero essere concatenati ad altre vulnerabilità per compromettere la funzionalità dell'utente. Nel tempo, potrebbero emergere anche nuove tecniche di exploit che aumentano il rischio di queste vulnerabilità. Seguendo i principi di sicurezza standard, correggi queste vulnerabilità per mantenere un ambiente sicuro.

Correzione: aggiorna le funzioni interessate

Consultate la sezione Riferimenti nella scheda Vulnerabilità per conoscere la caratteristica. La documentazione del fornitore potrebbe includere linee guida specifiche per la correzione. Aggiorna le librerie vulnerabili alle versioni sicure più recenti seguendo le procedure consigliate dal fornitore.

In genere, il flusso di lavoro di riparazione dipende dal fatto che il pacchetto Lambda sia stato distribuito caricando un file zip o creando una funzione Lambda con un'immagine del contenitore. Dopo aver aggiornato le librerie, aggiorna il codice della funzione Lambda per utilizzare la versione fissa. Successivamente, distribuisci la versione aggiornata.

La funzione Lambda contiene pacchetti software dannosi

I pacchetti dannosi sono componenti software che contengono codice dannoso progettato per compromettere la riservatezza, l'integrità e la disponibilità dei sistemi e dei dati. I pacchetti dannosi

rappresentano una minaccia attiva e critica per la funzione Lambda, poiché gli aggressori possono eseguire codice dannoso automaticamente senza sfruttare una vulnerabilità. Seguendo le best practice di sicurezza, rimuovi i pacchetti dannosi per proteggere la funzione Lambda da potenziali attacchi.

Correzione: rimuovi i pacchetti dannosi

Esamina i dettagli del pacchetto dannoso nella sezione Riferimenti della scheda Vulnerabilità della caratteristica per comprendere la minaccia. Rimuovi i pacchetti dannosi identificati dal codice della funzione e dalle dipendenze. Per le funzioni che utilizzano livelli, controlla se i pacchetti dannosi sono installati in qualsiasi livello e rimuovili.

Aggiorna il pacchetto di distribuzione o l'immagine del contenitore per escludere i pacchetti dannosi, quindi distribuisci la versione aggiornata. Per istruzioni, consulta Implementazione delle funzioni Lambda come archivi di file.zip per archivi di file.zip o Creazione di una funzione Lambda utilizzando un'immagine del contenitore per le immagini del contenitore.

La funzione Lambda presenta vulnerabilità nel codice

Il codice dell'applicazione della funzione Lambda contiene vulnerabilità di sicurezza che potrebbero essere sfruttate dagli autori delle minacce. Le vulnerabilità del codice includono fughe di dati, difetti di iniezione, crittografia mancante e crittografia debole che vengono identificate tramite l'analisi automatizzata del codice. Queste vulnerabilità rappresentano rischi per la sicurezza AWS dell'ambiente, in quanto gli aggressori possono sfruttarle per compromettere la riservatezza, l'integrità o la disponibilità dei dati o per accedere ad altri sistemi. Le vulnerabilità del codice rappresentano punti deboli di sicurezza che potrebbero essere concatenati ad altri vettori di attacco per compromettere la funzionalità dell'utente. Seguendo le migliori pratiche di sicurezza, risolvi queste vulnerabilità del codice per proteggere la funzione dagli attacchi.

Correzione: aggiorna le funzioni interessate

Esamina la sezione Riferimenti nella scheda Vulnerabilità della caratteristica. I risultati di Amazon Inspector possono includere linee guida specifiche per la correzione e frammenti di codice che mostrano le posizioni dei codici vulnerabili. Risolvi i problemi di sicurezza identificati nel codice della funzione utilizzando i blocchi di codice plug-and-play forniti o implementando pratiche di codifica sicure.

Esamina sempre i suggerimenti per la correzione del codice prima di adottarli, poiché potrebbe essere necessario modificarli per garantire che il codice funzioni come previsto. Dopo aver corretto le vulnerabilità, aggiorna il codice della funzione Lambda per utilizzare la versione corretta. Per

istruzioni, consulta Aggiornamento del codice della funzione nella Guida per gli AWS Lambda sviluppatori.

Successivamente, distribuisci la versione aggiornata. Per istruzioni, consulta Implementazione delle funzioni Lambda come archivi di file.zip per archivi di file.zip o Creazione di una funzione Lambda utilizzando un'immagine del contenitore per le immagini del contenitore. Per ulteriori informazioni sulla scansione del codice di Amazon Inspector, consulta la scansione del codice Amazon Inspector Lambda nella Amazon Inspector User Guide.

Caratteristiche di impatto per le funzioni Lambda

I tratti di impatto descrivono il potenziale raggio di esplosione di un'esposizione. Security Hub analizza le autorizzazioni effettive del AWS Identity and Access Management principale associato alla funzione Lambda per determinare le risorse a valle che un utente malintenzionato potrebbe raggiungere se la funzione viene compromessa, nonché la criticità aziendale di tali risorse. Ogni caratteristica di impatto identifica uno specifico modello di escalation dei privilegi. Per ridurre il raggio d'azione, esaminate i percorsi di autorizzazione descritti in ogni caratteristica e rimuovete eventuali privilegi non necessari.

Seguendo i principi di sicurezza standard, concedi il privilegio minimo fornendo solo le autorizzazioni necessarie per eseguire un'attività. Sostituisci politiche generali con politiche circoscritte che garantiscano solo le azioni e le risorse specifiche necessarie. Per identificare le autorizzazioni non utilizzate da rimuovere, utilizza IAM Access Analyzer per generare consigli basati sulla cronologia degli accessi. Per ulteriori informazioni, consulta Findings for external and inused access e Apply least-privilege permissions nella IAM User Guide.

Dispone di un percorso di esecutore privilegiato con pieno controllo

Il principale associato può passare un ruolo e inserire codice in una risorsa di calcolo che dispone già di autorizzazioni elevate. Ciò consente al principale di ottenere il pieno controllo sull'esecutore ed eseguire qualsiasi azione consentita dal ruolo dell'esecutore.

Ha un percorso diretto di escalation delle politiche

Il principale associato può modificare direttamente le politiche IAM per concedersi autorizzazioni aggiuntive, aumentando i propri privilegi senza risorse intermedie.

Ha un percorso di dirottamento delle politiche di fiducia

Il principale associato può modificare la politica di fiducia di un ruolo IAM per consentirsi di assumere quel ruolo, ottenendo le autorizzazioni del ruolo.

Ha un percorso di ransomware per i dati

Il principale associato può crittografare o eliminare i dati in un modo che potrebbe essere utilizzato per il ransomware, ad esempio crittografando gli oggetti Amazon S3 con una AWS KMS chiave gestita dal cliente e quindi modificando la politica della chiave.

Ha un percorso di rimozione della restrizione

Il principale associato può rimuovere le restrizioni di sicurezza come i limiti di autorizzazione, le politiche di controllo dei servizi o le dichiarazioni di rifiuto delle politiche basate sulle risorse, ampliando le funzionalità che possono fare gli altri principali o la risorsa stessa.

Ha il percorso pass role create executor

Il principale associato può creare una nuova risorsa di calcolo (come una funzione Lambda o un'istanza Amazon EC2) e assegnarle un ruolo privilegiato, riciclando efficacemente le proprie autorizzazioni attraverso la nuova risorsa.

Ha un percorso di esecuzione esistente di Swap Role

Il principale associato può modificare il ruolo IAM associato a una risorsa di elaborazione esistente, sostituendolo con un ruolo più privilegiato per aumentare l'accesso.

Ha un percorso di escalation della catena di ruoli

Il principale associato può assumere una sequenza di ruoli, in cui ogni ruolo della catena dispone di autorizzazioni progressivamente più ampie, fino a raggiungere infine un ruolo altamente privilegiato.

Dispone di un percorso di esecutore privilegiato per il codice di iniezione

Il principale associato può iniettare codice in una risorsa di elaborazione in esecuzione che dispone di autorizzazioni elevate, eseguendo operazioni arbitrarie nell'ambito del ruolo privilegiato di tale risorsa.

Ha disabilitato il percorso di audit trail

Il responsabile associato può disabilitare i servizi di registrazione o monitoraggio CloudTrail, ad esempio coprire efficacemente le tracce durante o dopo un'escalation.

Ha accesso al percorso dell'esecutore esistente

Il principale associato può richiamare o connettersi a una risorsa di elaborazione esistente e utilizzare il ruolo associato per eseguire azioni privilegiate.

Dispone di un percorso di coniazione delle credenziali

Il principale associato può creare nuove credenziali a lungo termine (come chiavi di accesso o profili di accesso) per altri principali, stabilendo percorsi di accesso persistenti che sopravvivono alla rotazione delle password o alle scadenze delle sessioni.

Dispone di un percorso di accesso ai dati di tipo pass role

Il responsabile associato può creare una risorsa di servizio e assegnarle un ruolo con accesso a dati sensibili, ottenendo l'accesso indiretto a tali dati tramite la nuova risorsa.

Ha un percorso di dirottamento del ruolo

Il principale associato può passare un ruolo a un'attività pianificata o basata su eventi (come una funzione Lambda attivata da un evento), consentendogli di eseguire codice arbitrario con le autorizzazioni di quel ruolo.

Ha un percorso di accesso ai dati a hop singolo

Il principale associato può accedere direttamente alle risorse di dati sensibili (come i bucket Amazon S3 o le tabelle DynamoDB) tramite le autorizzazioni esistenti, senza bisogno di passaggi di escalation intermedi.

Ha un percorso di avanzamento delle capacità

Il principale associato dispone di un percorso di assegnazione dei privilegi che ne migliora le capacità complessive oltre a quanto suggerirebbe l'assegnazione diretta delle autorizzazioni. Questa è una classificazione generale per i percorsi che non corrispondono a uno schema più specifico.

Criticità aziendale

La criticità aziendale della risorsa principale, stabilita dalle regole di automazione o dall'inferenza del nome e dei tag.

Correzione delle esposizioni per istanze e cluster Amazon RDS

AWS Security Hub può generare risultati sull'esposizione per istanze e cluster Amazon RDS.

Sulla console Security Hub, l'istanza o il cluster Amazon RDS coinvolto nella rilevazione dell'esposizione e le relative informazioni identificative sono elencati nella sezione Risorse dei

dettagli dei risultati. A livello di programmazione, puoi recuperare i dettagli delle risorse con il GetFindingsV2 funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la risoluzione fornite in questo argomento potrebbero richiedere ulteriori consultazioni in altre risorse. AWS

Indice

- Caratteristiche di configurazione errata per istanze e cluster Amazon RDS
  - L'istanza DB di Amazon RDS è configurata con accesso pubblico
  - Il cluster Amazon RDS DB ha un'istantanea condivisa pubblicamente
  - L'istanza DB di Amazon RDS ha un'istantanea condivisa pubblicamente
  - L'istanza DB di Amazon RDS ha un'istantanea non crittografata a riposo
  - Il cluster DB Amazon RDS ha un'istantanea non crittografata a riposo
  - L'istanza DB di Amazon RDS ha un gruppo di sicurezza aperto
  - L'istanza DB di Amazon RDS ha l'autenticazione del database IAM disabilitata
  - L'istanza DB di Amazon RDS utilizza il nome utente amministratore predefinito
  - Il cluster DB Amazon RDS utilizza il nome utente di amministratore predefinito
  - L'istanza DB di Amazon RDS ha gli aggiornamenti automatici delle versioni secondarie disattivati
  - L'istanza DB di Amazon RDS ha i backup automatici disattivati
  - L'istanza DB di Amazon RDS ha la protezione dalle eliminazioni disattivata
  - Il cluster DB Amazon RDS ha la protezione dalle eliminazioni disattivata
  - L'istanza DB di Amazon RDS utilizza la porta predefinita per il motore di database

- L'istanza DB di Amazon RDS non è coperta da un piano di backup
- Caratteristiche dei dati sensibili per le istanze DB di Amazon RDS
  - L'istanza DB di Amazon RDS contiene dati sensibili

Caratteristiche di configurazione errata per istanze e cluster Amazon RDS

Di seguito vengono descritte le caratteristiche di configurazione errata e le fasi di correzione per le istanze e i cluster Amazon RDS.

L'istanza DB di Amazon RDS è configurata con accesso pubblico

Le istanze Amazon RDS con accesso pubblico sono potenzialmente accessibili su Internet tramite i relativi endpoint. Sebbene l'accesso pubblico sia talvolta necessario per esempio per la funzionalità, questa configurazione può essere utilizzata come potenziale vettore di attacco per consentire agli utenti non autorizzati di tentare di accedere al database. I database accessibili al pubblico possono essere esposti a scansioni delle porte, attacchi di forza bruta e tentativi di sfruttamento. Seguendo i principi di sicurezza standard, limita l'esposizione pubblica delle risorse del database.

Soluzione: modifica le impostazioni di accesso pubblico

Nella rilevazione dell'esposizione, scegli il link alla risorsa. L'istanza DB interessata viene aperta nella console di Amazon RDS. Valuta se l'istanza DB richiede l'accessibilità pubblica in base all'architettura dell'applicazione. Per ulteriori informazioni, consulta Configurazione dell'accesso pubblico o privato in Amazon RDS.

Il cluster Amazon RDS DB ha un'istantanea condivisa pubblicamente

Le istantanee pubbliche sono accessibili da chiunque Account AWS, esponendo potenzialmente i dati sensibili a utenti non autorizzati. Chiunque Account AWS è autorizzato a copiare queste istantanee pubbliche e a crearne istanze DB, il che potrebbe comportare violazioni dei dati o accessi non autorizzati ai dati. Seguendo le migliori pratiche di sicurezza, limita l'accesso agli snapshot di Amazon RDS solo alle organizzazioni affidabili. Account AWS

Soluzione: configura uno snapshot di Amazon RDS per l'accesso privato

Nella ricerca dell'esposizione, apri la risorsa tramite il collegamento ipertestuale. Per informazioni su come modificare le impostazioni di condivisione delle istantanee, consulta Sharing a snapshot nella Amazon Aurora User Guide. Per informazioni su come interrompere la condivisione di istantanee, consulta Interruzione della condivisione di istantanee nella Amazon Aurora User Guide. .

L'istanza DB di Amazon RDS ha un'istantanea condivisa pubblicamente

Le istantanee pubbliche sono accessibili da chiunque Account AWS, esponendo potenzialmente i dati sensibili a utenti non autorizzati. Chiunque Account AWS è autorizzato a copiare queste istantanee pubbliche e a crearne istanze DB, il che potrebbe comportare violazioni dei dati o accessi non autorizzati ai dati. Seguendo le migliori pratiche di sicurezza, limita l'accesso agli snapshot di Amazon RDS solo alle organizzazioni affidabili. Account AWS

Soluzione: configura uno snapshot di Amazon RDS per l'accesso privato

Nella ricerca dell'esposizione, apri la risorsa tramite il collegamento ipertestuale. Per informazioni su come modificare le impostazioni di condivisione delle istantanee, consulta Sharing a DB snapshot nella Amazon RDS User Guide. Per informazioni su come interrompere la condivisione di istantanee, consulta Stop sharing a DB snapshot nella Amazon RDS User Guide. .

L'istanza DB di Amazon RDS ha un'istantanea non crittografata a riposo

Le istantanee delle istanze DB Amazon RDS non crittografate possono esporre dati sensibili se si ottiene un accesso non autorizzato al livello di storage. Senza crittografia, i dati contenuti nelle istantanee potrebbero essere esposti tramite accessi non autorizzati. Ciò comporta il rischio di violazioni dei dati e della conformità. Seguendo le migliori pratiche di sicurezza, crittografa tutte le risorse del database e i relativi backup per mantenere la riservatezza dei dati.

Soluzione: aggiornamento delle risorse interessate

Nella rilevazione dell'esposizione, scegli il link alla risorsa. Verrà aperta l'istantanea interessata nella console Amazon RDS. Non è possibile crittografare direttamente un'istantanea non crittografata esistente.

Create invece una copia crittografata dell'istantanea non crittografata. Per istruzioni dettagliate, consulta la sezione DB Cluster Snapshot Copying and Encrypting Amazon RDS resources nella Amazon Aurora User Guide.

Il cluster DB Amazon RDS ha un'istantanea non crittografata a riposo

Le istantanee del cluster DB Amazon RDS non crittografate possono esporre dati sensibili se si ottiene un accesso non autorizzato al livello di storage. Senza crittografia, i dati contenuti nelle istantanee potrebbero essere esposti tramite accessi non autorizzati. Ciò comporta il rischio di violazioni dei dati e della conformità. Seguendo le migliori pratiche di sicurezza, crittografa tutte le risorse del database e i relativi backup per mantenere la riservatezza dei dati.

Correzione: crea una copia crittografata dell'istantanea

Nella ricerca dell'esposizione, scegli il link alla risorsa. Verrà aperta l'istantanea interessata nella console Amazon RDS. Non è possibile crittografare direttamente un'istantanea non crittografata esistente.

Create invece una copia crittografata dell'istantanea non crittografata. Per istruzioni dettagliate, consulta la sezione DB Cluster Snapshot Copying and Encrypting Amazon RDS resources nella Amazon Aurora User Guide.

L'istanza DB di Amazon RDS ha un gruppo di sicurezza aperto

I gruppi di sicurezza fungono da firewall virtuali per le istanze Amazon RDS per controllare il traffico in entrata e in uscita. I gruppi di sicurezza aperti, che consentono l'accesso illimitato da qualsiasi indirizzo IP, possono esporre le istanze del database ad accessi non autorizzati e potenziali attacchi. Seguendo i principi di sicurezza standard, limita l'accesso dei gruppi di sicurezza a porte e indirizzi IP specifici per mantenere il principio del privilegio minimo.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi le regole del gruppo di sicurezza e valuta la configurazione corrente

Nel rilevamento dell'esposizione, apri la risorsa per il gruppo di sicurezza dell'istanza DB. Valuta quali porte sono aperte e accessibili da ampi intervalli di IP, ad esempio`(0.0.0.0/0 or ::/0)`. Per informazioni sulla visualizzazione dei dettagli dei gruppi di sicurezza, DescribeSecurityGroups consulta Amazon Elastic Compute Cloud API Reference.

Modifica le regole del gruppo di sicurezza

Modifica le regole del tuo gruppo di sicurezza per limitare l'accesso a specifici indirizzi o intervalli IP affidabili. Quando aggiorni le regole del tuo gruppo di sicurezza, valuta la possibilità di separare i requisiti di accesso per i diversi segmenti di rete creando regole per ogni intervallo IP di origine richiesto o limitando l'accesso a porte specifiche. Per modificare le regole dei gruppi di sicurezza, consulta Configurare le regole dei gruppi di sicurezza nella Amazon EC2 User Guide. Per modificare la porta predefinita di un'istanza di database Amazon RDS esistente, consulta Modificare il cluster DB utilizzando la console, l'interfaccia a riga di comando e l'API nella Amazon Aurora User Guide.

L'istanza DB di Amazon RDS ha l'autenticazione del database IAM disabilitata

L'autenticazione del database IAM ti consente di autenticarti nel tuo database Amazon RDS utilizzando le credenziali IAM anziché le password del database. Ciò offre diversi vantaggi in

termini di sicurezza, come la gestione centralizzata degli accessi, le credenziali temporanee e l'eliminazione della memorizzazione delle password del database nel codice dell'applicazione. L'autenticazione del database IAM consente l'autenticazione alle istanze del database con un token di autenticazione anziché una password. Di conseguenza, il traffico di rete da e verso l'istanza del database viene crittografato tramite SSL. Senza l'autenticazione IAM, i database si affidano in genere all'autenticazione basata su password, che può portare al riutilizzo delle password e a password deboli. Seguendo le migliori pratiche di sicurezza, abilita l'autenticazione del database IAM.

Soluzione: abilita l'autenticazione del database IAM

Nella ricerca dell'esposizione, scegli il link alla risorsa. L'istanza DB interessata viene aperta nella console di Amazon RDS. Puoi abilitare l'autenticazione del database IAM nelle opzioni del database.

Per ulteriori informazioni, consulta Abilitare e disabilitare l'autenticazione del database IAM nella Amazon RDS User Guide. Dopo aver abilitato l'autenticazione IAM, aggiorna le istanze DB per utilizzare l'autenticazione IAM anziché l'autenticazione basata su password.

L'istanza DB di Amazon RDS utilizza il nome utente amministratore predefinito

L'utilizzo di nomi utente predefiniti (ad esempio, «admin», «root») per le istanze DB aumenta il rischio di sicurezza in quanto sono ampiamente noti e comunemente presi di mira dagli attacchi di forza bruta. I nomi utente predefiniti sono prevedibili e facilitano il tentativo di accesso al database da parte di utenti non autorizzati. Con i nomi utente predefiniti, gli aggressori devono solo ottenere le password anziché utilizzare entrambe per accedere al database. Seguendo le best practice di sicurezza, utilizza nomi utente di amministratore univoci per l'istanza del database per migliorare la sicurezza attraverso l'oscurità e ridurre il rischio di tentativi di accesso non autorizzati.

Soluzione: configura un nome utente amministratore univoco

Nella ricerca dell'esposizione, scegli il link alla risorsa. L'istanza DB interessata viene aperta nella console di Amazon RDS. Non è possibile modificare il nome utente dell'amministratore di un'istanza DB Amazon RDS esistente. Per creare un nome di amministratore univoco, devi creare una nuova istanza DB con un nome utente personalizzato e migrare i tuoi dati.

Il cluster DB Amazon RDS utilizza il nome utente di amministratore predefinito

L'utilizzo di nomi utente predefiniti (ad esempio, «admin», «root») per le istanze DB aumenta il rischio di sicurezza in quanto sono ampiamente noti e comunemente presi di mira dagli attacchi di forza bruta. I nomi utente predefiniti sono prevedibili e facilitano il tentativo di accesso al database da parte di utenti non autorizzati. Con i nomi utente predefiniti, gli aggressori devono solo ottenere le password

anziché utilizzare entrambe per accedere al database. Seguendo le best practice di sicurezza, utilizza nomi utente di amministratore univoci per l'istanza del database per migliorare la sicurezza attraverso l'oscurità e ridurre il rischio di tentativi di accesso non autorizzati.

Soluzione: configura un nome utente amministratore univoco

Nella ricerca dell'esposizione, scegli il link alla risorsa. L'istanza DB interessata viene aperta nella console di Amazon RDS. Non è possibile modificare il nome utente dell'amministratore di un'istanza DB Amazon RDS esistente. Per creare un nome di amministratore univoco, devi creare una nuova istanza DB con un nome utente personalizzato e migrare i tuoi dati.

L'istanza DB di Amazon RDS ha gli aggiornamenti automatici delle versioni secondarie disattivati

Gli aggiornamenti automatici delle versioni secondarie assicurano che le istanze Amazon RDS ricevano automaticamente aggiornamenti delle versioni minori del motore quando diventano disponibili. Questi aggiornamenti spesso includono importanti patch di sicurezza e correzioni di bug che aiutano a mantenere la sicurezza e la stabilità del database. Il database rischia di funzionare con vulnerabilità di sicurezza note che sono state corrette nelle versioni secondarie più recenti. Senza aggiornamenti automatici, le istanze del database possono accumulare vulnerabilità di sicurezza man mano che vengono scoperti nuovi CVE. Seguendo le migliori pratiche di sicurezza, abilita gli aggiornamenti automatici delle versioni secondarie per tutte le istanze Amazon RDS.

Soluzione: abilita gli aggiornamenti automatici delle versioni secondarie

Nella ricerca dell'esposizione, scegli il link alla risorsa. L'istanza DB interessata viene aperta nella console di Amazon RDS. Puoi visualizzare le impostazioni automatiche di upgrade secondario nella scheda Manutenzione e backup.

Per ulteriori informazioni, consulta Aggiornamenti automatici delle versioni secondarie di Amazon RDS for MySQL. Puoi anche configurare la finestra di manutenzione in modo che si verifichi durante i periodi di scarsa attività del database.

L'istanza DB di Amazon RDS ha i backup automatici disattivati

I backup automatici forniscono un ripristino point-in-time per le istanze Amazon RDS, consentendoti di ripristinare il database in qualsiasi momento entro il periodo di conservazione. Quando i backup automatici sono disattivati, rischi di perdere i dati in caso di eliminazione dolosa, danneggiamento dei dati o altri scenari di perdita dei dati. In caso di attività dannose come attacchi ransomware, cancellazione delle tabelle del database o danneggiamento, la capacità di ripristinare un punto temporale precedente all'incidente riduce il tempo necessario per il ripristino da un

incidente. Seguendo le migliori pratiche di sicurezza, abilita i backup automatici con un periodo di conservazione appropriato per tutti i database di produzione.

L'istanza DB di Amazon RDS ha la protezione dalle eliminazioni disattivata

La protezione dall'eliminazione del database è una funzionalità che aiuta a prevenire l'eliminazione delle istanze di database. Quando la protezione dall'eliminazione è disattivata, il database può essere eliminato da qualsiasi utente con autorizzazioni sufficienti, con conseguente potenziale perdita di dati o tempi di inattività delle applicazioni. Gli aggressori possono eliminare il database, con conseguenti interruzioni del servizio, perdita di dati e aumento dei tempi di ripristino. Seguendo le best practice di sicurezza, abilita la protezione dall'eliminazione per le tue istanze DB RDS per impedirne l'eliminazione dannosa.

Soluzione: abilita la protezione dall'eliminazione per il tuo cluster DB Amazon RDS

Nella ricerca dell'esposizione, scegli il link alla risorsa. Questo apre il cluster DB interessato.

Il cluster DB Amazon RDS ha la protezione dalle eliminazioni disattivata

La protezione dall'eliminazione del database è una funzionalità che aiuta a prevenire l'eliminazione delle istanze del database. Quando la protezione dall'eliminazione è disattivata, il database può essere eliminato da qualsiasi utente con autorizzazioni sufficienti, con conseguente potenziale perdita di dati o tempi di inattività delle applicazioni. Gli aggressori possono eliminare il database, con conseguenti interruzioni del servizio, perdita di dati e aumento dei tempi di ripristino. Seguendo le migliori pratiche di sicurezza, abilita la protezione dall'eliminazione per i tuoi cluster RDS DB per prevenire eliminazioni dannose.

Soluzione: abilita la protezione dall'eliminazione per il tuo cluster DB Amazon RDS

Nella ricerca dell'esposizione, scegli il link alla risorsa. Questo apre il cluster DB interessato.

L'istanza DB di Amazon RDS utilizza la porta predefinita per il motore di database

Le istanze Amazon RDS che utilizzano porte predefinite per i motori di database possono essere esposte a maggiori rischi di sicurezza, in quanto queste porte predefinite sono ampiamente note e sono spesso prese di mira da strumenti di scansione automatici. La modifica dell'istanza DB per utilizzare porte non predefinite aggiunge un ulteriore livello di sicurezza attraverso l'oscurità, rendendo più difficile per gli utenti non autorizzati eseguire attacchi automatici o mirati al database. Le porte predefinite vengono in genere scansionate da persone non autorizzate e possono far sì che l'istanza DB venga presa di mira. Seguendo le best practice di sicurezza, modifica la porta predefinita con una porta personalizzata per ridurre il rischio di attacchi automatici o mirati.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Aggiorna le risorse interessate

Nella rilevazione dell'esposizione, scegli il link alla risorsa. L'istanza DB interessata viene aperta nella console di Amazon RDS.

Aggiorna le stringhe di connessione dell'applicazione

Dopo aver modificato la porta, aggiorna tutte le applicazioni e i servizi che si connettono alla tua istanza Amazon RDS per utilizzare il nuovo numero di porta.

L'istanza DB di Amazon RDS non è coperta da un piano di backup

AWS Backup è un servizio di backup completamente gestito che centralizza e automatizza il backup dei dati tra di loro. Servizi AWS Se l'istanza DB non è coperta da un piano di backup, rischi di perdere i dati in caso di eliminazione dolosa, danneggiamento dei dati o altri scenari di perdita dei dati. In caso di attività dannose come attacchi ransomware, cancellazione delle tabelle del database o danneggiamento, la capacità di ripristinare un punto temporale precedente all'incidente riduce il tempo necessario per il ripristino da un incidente. Seguendo le best practice di sicurezza, includi le tue istanze Amazon RDS in un piano di backup per garantire la protezione dei dati.

Soluzione: crea e assegna un piano di backup per la tua istanza DB

Nella ricerca dell'esposizione, scegli il link alla risorsa. L'istanza DB interessata viene aperta nella console di Amazon RDS. Valuta quali sono la frequenza di backup, il periodo di conservazione e le regole del ciclo di vita migliori per le tue applicazioni.

Caratteristiche dei dati sensibili per le istanze DB di Amazon RDS

Ecco le caratteristiche dei dati sensibili per le istanze DB di Amazon RDS e i passaggi di riparazione suggeriti.

L'istanza DB di Amazon RDS contiene dati sensibili

Una scansione di sicurezza dei dati ha confermato la presenza di record sensibili nell'istanza DB di Amazon RDS. Un prodotto integrato per la sicurezza dei dati imposta questa caratteristica quando ispeziona il contenuto dell'istanza DB e identifica i record che richiedono protezione.

La presenza di dati sensibili aumenta l'impatto di ogni altra debolezza sulla stessa istanza DB. Un percorso di rete o una configurazione di accesso permissivo che altrimenti esporrebbe i dati delle applicazioni espone invece record regolamentati o riservati. Un aggressore che raggiunge l'istanza DB può interrogare e copiare tali record in blocco e conservarli all'esterno dell'ambiente. L'autore della minaccia può anche utilizzare qualsiasi credenziale recuperata per autenticarsi su altri sistemi. Seguendo le migliori pratiche di sicurezza, consigliamo di limitare l'accesso alla rete e all'identità alle istanze DB di Amazon RDS che archiviano record sensibili e di crittografare tali record a riposo e in transito.

I dati sensibili possono includere:

- Credenziali, ad esempio password, chiavi di accesso e stringhe di connessione
- Informazioni di identificazione personale
- Informazioni finanziarie, come numeri di conto e dati delle carte di pagamento
- Contenuti riservati che richiedono protezione

La rimozione dei record sensibili è l'unico modo per eliminare questa caratteristica. Se il carico di lavoro richiede l'istanza DB per archiviare dati sensibili, le seguenti best practice di sicurezza riducono il rischio di esposizione.

Esamina i dati sensibili sull'istanza DB

Nella ricerca dell'esposizione, apri la risorsa con il collegamento ipertestuale. Questo apre l'istanza DB interessata. Annota l'identificatore dell'istanza DB e registra i gruppi di sicurezza VPC elencati in Connettività e sicurezza. Esamina i risultati sulla sicurezza dei dati che hanno riportato i record sensibili per determinare quali database, schemi e tabelle li contengono.

In base al tipo di dati sensibili rilevati, implementa i controlli di sicurezza appropriati:

- Limita l'accesso alla rete in entrata: nella console Amazon RDS, scegli Database, seleziona l'istanza DB e scegli Connettività e sicurezza. Apri ogni gruppo di sicurezza VPC collegato e rivedi le relative regole in entrata. Sostituisci qualsiasi regola che consenta la porta del database da `0.0.0.0/0` o `::/0` con gli intervalli CIDR o gli ID dei gruppi di sicurezza specifici utilizzati dalle tue applicazioni. Per ulteriori informazioni, consulta Controllo dell'accesso con i gruppi di sicurezza nella Guida per l'utente di Amazon RDS.
- Rimuovi l'accessibilità pubblica: nella console Amazon RDS, seleziona l'istanza DB, scegli Modifica e in Connettività imposta Accesso pubblico su Non accessibile pubblicamente. Posiziona l'istanza DB in sottoreti private che non hanno alcun percorso verso un gateway Internet.

Raggiungila dalle tue applicazioni tramite VPC, AWS Direct Connect o una connessione VPN. Per ulteriori informazioni, consulta la sezione Working with a DB instance in a VPC (Utilizzo di un'istanza database in un VPC) nella Guida per l'utente di Amazon RDS.

- Limita chi può autenticarsi nel database: concedi a ciascuna applicazione e utente solo i privilegi del database necessari per il suo funzionamento. Revoca l'accesso in lettura alle tabelle che contengono record sensibili a qualsiasi utente del database che non ne abbia bisogno. Usa l'autenticazione del database IAM in modo che le identità IAM e i token di breve durata controllino l'accesso anziché le password a lunga durata del database. Per ulteriori informazioni, consulta l'autenticazione del database IAM nella Amazon RDS User Guide.
- Crittografa i record sensibili a riposo: nella console Amazon RDS, seleziona l'istanza DB e scegli la scheda Configurazione per verificare se l'istanza DB utilizza la crittografia. Non è possibile abilitare la crittografia a riposo su un'istanza DB non crittografata esistente. Per crittografarne i dati, crea un'istantanea dell'istanza DB. Copia l'istantanea e seleziona una chiave AWS KMS per la copia, quindi ripristina la copia istantanea crittografata in una nuova istanza DB. Reindirizza le applicazioni sul nuovo endpoint ed elimina l'istanza DB non crittografata e le relative istantanee. Per ulteriori informazioni, consulta la sezione Encrypting Amazon RDS resources nella Amazon RDS User Guide.
- Richiedi la crittografia in transito: configura i client del database con cui connettersi SSL/TLS utilizzando il pacchetto di certificati Amazon RDS. Applica le connessioni crittografate sull'istanza DB tramite il parametro fornito a tale scopo dal motore del database. Per ulteriori informazioni, consulta Using SSL/TLS to encrypt a connection to a an db instance o cluster nella Amazon RDS User Guide.
- Monitora l'accesso all'istanza DB: pubblica i log del motore di database su Amazon CloudWatch Logs ed esaminali per le connessioni da fonti impreviste e per le query sulle tabelle che contengono record sensibili. Per ulteriori informazioni, consulta Monitoring Amazon RDS log file nella Amazon RDS User Guide.

Correzione delle esposizioni per i bucket Amazon S3

AWS Security Hub può generare risultati sull'esposizione per i bucket Amazon Simple Storage Service (Amazon S3).

Sulla console Security Hub, il bucket Amazon S3 coinvolto nella rilevazione dell'esposizione e le relative informazioni identificative sono elencati nella sezione Risorse dei dettagli dei risultati. A livello di programmazione, puoi recuperare i dettagli delle risorse con il GetFindingsV2 funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la risoluzione fornite in questo argomento potrebbero richiedere ulteriori consultazioni in altre risorse. AWS

Indice

- Caratteristiche di configurazione errata per i bucket Amazon S3
  - Il controllo delle versioni del bucket Amazon S3 è disabilitato
  - Il bucket Amazon S3 ha Object Lock disabilitato
  - Il bucket Amazon S3 non è crittografato a riposo con AWS KMS keys
  - Multi-factor l'eliminazione dell'autenticazione (MFA) è disabilitata su un bucket Amazon S3 con versione
  - Il bucket Amazon S3 consente ai principali di altri AWS account per modificare le autorizzazioni del bucket
- Caratteristiche di raggiungibilità per i bucket Amazon S3
  - Il bucket Amazon S3 ha accesso in lettura pubblico
  - Il bucket Amazon S3 ha accesso pubblico in scrittura
- Caratteristiche dei dati sensibili per i bucket Amazon S3
  - Il bucket Amazon S3 contiene dati sensibili

Caratteristiche di configurazione errata per i bucket Amazon S3

Ecco le caratteristiche di configurazione errata per i bucket Amazon S3 e le procedure di correzione suggerite.

Il controllo delle versioni del bucket Amazon S3 è disabilitato

Amazon S3 Versioning ti aiuta a mantenere più varianti di un oggetto nello stesso bucket. Quando il controllo delle versioni è disabilitato, Amazon S3 memorizza solo la versione più recente di ciascun oggetto, il che significa che se gli oggetti vengono eliminati o sovrascritti accidentalmente o intenzionalmente, non possono essere recuperati. Versioning-enabled i bucket forniscono protezione contro l'eliminazione accidentale, i guasti delle applicazioni e gli incidenti di sicurezza come gli attacchi ransomware, in cui potrebbero verificarsi modifiche o cancellazioni non autorizzate dei dati. Seguendo le migliori pratiche di sicurezza, abilita il controllo delle versioni per i bucket contenenti dati importanti che sarebbero difficili o impossibili da ricreare in caso di perdita.

Soluzione: abilita il controllo delle versioni

Per abilitare il controllo delle versioni di Amazon S3 su un bucket, consulta Enabling versioning on buckets nella Amazon S3 User Guide. Quando abiliti il controllo delle versioni, prendi in considerazione l'implementazione di regole del ciclo di vita per gestire lo storage, poiché il controllo delle versioni manterrà più copie degli oggetti.

Il bucket Amazon S3 ha Object Lock disabilitato

Amazon S3 Object Lock fornisce un modello worm (write-once-read-many) per gli oggetti Amazon S3, che impedisce che vengano eliminati o sovrascritti per un periodo fisso o indefinito. Quando Object Lock è disabilitato, i tuoi oggetti potrebbero essere vulnerabili all'eliminazione, alla modifica o alla crittografia accidentali o dolose da parte del ransomware. Object Lock è particolarmente importante per la conformità ai requisiti normativi che richiedono l'archiviazione immutabile dei dati e per la protezione da minacce sofisticate come il ransomware che potrebbe tentare di crittografare i dati. Abilitando Object Lock, puoi applicare le politiche di conservazione come ulteriore livello di protezione dei dati e creare una strategia di backup immutabile per i tuoi dati critici. Seguendo le best practice di sicurezza, abilita Object Lock per impedire modifiche dannose ai tuoi oggetti.

Soluzione: configura S3 Object Lock

Nota che Object Lock può essere abilitato solo quando crei un nuovo bucket, quindi dovrai creare un nuovo bucket con Object Lock abilitato. Per migrazioni di grandi dimensioni, considera l'utilizzo di Batch Operations per copiare oggetti nel nuovo bucket. Prima di bloccare qualsiasi oggetto, devi anche abilitare Amazon S3 Versioning e Object Lock su un bucket. Poiché Object Lock può essere abilitato solo su nuovi bucket, dovrai migrare i dati esistenti in un nuovo bucket con Object Lock abilitato. Per informazioni su come configurare Object Lock su un bucket, consulta Configurazione di Amazon S3 Object Lock nella Amazon S3 User Guide. Dopo aver impostato Object Lock, scegli una modalità di conservazione appropriata in base al tuo ambiente.

Il bucket Amazon S3 non è crittografato a riposo con AWS KMS keys

Amazon S3 applica la crittografia lato server con le chiavi gestite da Amazon S3 come livello di crittografia predefinito per tutti i nuovi bucket. Sebbene le chiavi gestite di Amazon S3 offrano una solida protezione crittografica, non offrono lo stesso livello di controllo degli accessi e funzionalità di verifica delle chiavi. AWS Key Management Service Quando si utilizzano le chiavi KMS, l'accesso agli oggetti richiede le autorizzazioni sia per il bucket Amazon S3 che per la chiave KMS che ha crittografato l'oggetto. Ciò è particolarmente importante per i dati sensibili, per i quali è necessario un controllo granulare su chi può accedere agli oggetti crittografati e una registrazione di controllo completa dell'utilizzo delle chiavi di crittografia. Seguendo le migliori pratiche di sicurezza, utilizza le chiavi KMS per crittografare i bucket contenenti dati sensibili o per ambienti con severi requisiti di conformità.

Soluzione: configura la chiave bucket S3

Per configurare un bucket per utilizzare una chiave bucket Amazon S3 per nuovi oggetti, consulta Configurazione del bucket per l'utilizzo di una chiave bucket Amazon S3 per nuovi oggetti nella Amazon S3 User Guide. SSE-KMS Per informazioni su come crittografare un oggetto esistente, consulta Encrypting objects with Amazon S3 Batch Operations nel blog di storage. AWS

Quando implementi AWS KMS la crittografia, considera quanto segue:

- Gestione delle chiavi: decidi se utilizzare una chiave AWS gestita o una chiave gestita dal cliente (CMK). I CMK offrono ai clienti il pieno controllo sul ciclo di vita e sull'utilizzo delle proprie chiavi. Per ulteriori informazioni sulla differenza tra questi due tipi di chiavi, consulta le chiavi AWS KMS nella Developer Guide. AWS Key Management Service
- Rotazione delle chiavi: per ulteriori misure di sicurezza, abilita la rotazione automatica delle chiavi KMS. Per ulteriori informazioni, consulta Abilitare la rotazione automatica delle chiavi nella AWS Key Management Service Developer Guide.

Multi-factor l'eliminazione dell'autenticazione (MFA) è disabilitata su un bucket Amazon S3 con versione

Multi-factor l'eliminazione dell'autenticazione (MFA) fornisce un ulteriore livello di sicurezza per il tuo bucket Amazon S3. Richiede l'autenticazione a più fattori per le operazioni distruttive di Amazon S3. Quando l'eliminazione MFA è disabilitata, gli utenti con le autorizzazioni appropriate possono eliminare definitivamente le versioni degli oggetti o sospendere il controllo delle versioni sul bucket senza ulteriori problemi di autenticazione. L'attivazione dell'eliminazione MFA aiuta a proteggere i dati

dall'eliminazione non autorizzata o accidentale, fornendo una protezione avanzata contro attacchi ransomware, minacce interne ed errori operativi. L'eliminazione MFA è particolarmente utile per i bucket contenenti dati critici o sensibili alla conformità che devono essere protetti dall'eliminazione non autorizzata. Seguendo le best practice di sicurezza, abilita l'MFA per i tuoi bucket Amazon S3.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi i tipi di MFA

AWS supporta i seguenti tipi di MFA. Sebbene l'autenticazione con un dispositivo fisico fornisca in genere una protezione di sicurezza più rigorosa, l'utilizzo di qualsiasi tipo di MFA è più sicuro rispetto alla disattivazione dell'MFA.

Applica l'MFA a livello di politica delle risorse

Utilizza la chiave `aws:MultiFactorAuthAge` condizionale in una policy bucket per richiedere l'MFA per operazioni sensibili. Per ulteriori informazioni, consulta Requiring MFA nella Amazon S3 User Guide.

Abilitare MFA

Per abilitare l'eliminazione dell'MFA, assicurati innanzitutto che il controllo delle versioni sia abilitato sul tuo bucket Amazon S3. L'eliminazione MFA è supportata solo nei bucket in cui è abilitato il controllo delle versioni. Per informazioni su come abilitare il controllo delle versioni di Amazon S3, consulta Enabling versioning on buckets nella Amazon S3 User Guide. L'eliminazione MFA non può essere abilitata tramite la console Amazon S3. È necessario utilizzare l'API Amazon S3 o il. AWS CLI Per ulteriori informazioni, consulta Configurazione dell'eliminazione dell'MFA nella Guida per l'utente di Amazon S3.

Il bucket Amazon S3 consente ai principali di altri AWS account per modificare le autorizzazioni del bucket

Le policy dei bucket di Amazon S3 controllano l'accesso a bucket e oggetti. Quando le politiche dei bucket consentono ai principali di altri AWS account di modificare le autorizzazioni dei bucket, gli utenti non autorizzati possono riconfigurare il bucket. Se le credenziali principali esterne sono compromesse, gli utenti non autorizzati possono acquisire il controllo del bucket, con conseguenti violazioni dei dati o interruzioni del servizio. Seguendo i principi di sicurezza standard, limita le azioni di gestione delle autorizzazioni solo ai principali fidati.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi e identifica le politiche specifiche

Nell'esposizione, identifica il bucket Amazon S3 nel campo ARN. Nella console Amazon S3, seleziona il bucket e vai alla scheda Autorizzazioni per rivedere la policy del bucket. Rivedi la politica delle autorizzazioni allegata al bucket. Cerca le dichiarazioni politiche che prevedono azioni simili `s3:PutBucketPolicy, s3:PutBucketAcl, s3:DeleteBucketPolicy, s3:*` o le dichiarazioni politiche che consentono l'accesso ai principali utenti esterni al tuo account, come indicato nella dichiarazione principale.

Modifica la policy del bucket

Modifica la policy del bucket per rimuovere o limitare le azioni concesse ad altri AWS account:

- Rimuovi le dichiarazioni politiche che concedono azioni di gestione delle autorizzazioni agli account esterni.
- Se è richiesto l'accesso tra più account, sostituisci le autorizzazioni generiche (`s3:*`) con azioni specifiche che non includono la gestione delle autorizzazioni bucket.

Per informazioni sulla modifica di una policy bucket, consulta Aggiungere una policy bucket utilizzando la console Amazon S3 nella Amazon S3 User Guide.

Caratteristiche di raggiungibilità per i bucket Amazon S3

Ecco le caratteristiche di raggiungibilità per i bucket Amazon S3 e i passaggi di riparazione suggeriti.

Il bucket Amazon S3 ha accesso in lettura pubblico

I bucket Amazon S3 con accesso pubblico in lettura consentono a chiunque su Internet di visualizzare i contenuti del tuo bucket. Sebbene ciò possa essere necessario per siti Web accessibili al pubblico o risorse condivise, può creare rischi per la sicurezza se il bucket contiene dati sensibili. L'accesso pubblico in lettura può comportare la visualizzazione e il download non autorizzati, con conseguenti violazioni dei dati se i dati sensibili vengono archiviati in tali bucket. Seguendo i principi di sicurezza standard, limita l'accesso ai bucket Amazon S3 agli utenti e ai sistemi necessari.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Blocca l'accesso pubblico a livello di bucket

Amazon S3 fornisce impostazioni Block Public Access che possono essere configurate sia a livello di bucket che di account per impedire l'accesso pubblico indipendentemente dalle policy del bucket o dagli ACL. Per ulteriori informazioni, consulta Bloccare l'accesso pubblico allo storage Amazon S3 nella Amazon S3 User Guide. Dopo aver bloccato l'accesso pubblico, rivedi la configurazione di controllo degli accessi del bucket per assicurarti che sia in linea con i tuoi requisiti di accesso. Quindi rivedi la tua policy sui bucket di Amazon S3 per definire in modo esplicito chi può accedere al tuo bucket. Per esempi di politiche sui bucket, consulta Esempi di politiche sui bucket di Amazon S3 nella Amazon S3 User Guide.

Metodi di accesso alternativi

Se è richiesto l'accesso pubblico in lettura, considera queste alternative più sicure:

- Amazon CloudFront: utilizzalo CloudFront con Origin Access Identity (OAI) o Origin Access Control (OAC) per consentire l'accesso in lettura da un bucket Amazon S3 privato. Questa alternativa limita l'accesso diretto al tuo bucket Amazon S3, consentendo al contempo l'accesso pubblico ai contenuti tramite. CloudFront Per ulteriori informazioni, consulta Restricting access to an Amazon S3 origin nella Amazon Developer Guide. CloudFront
- URL prefirmati: utilizza URL prefirmati per l'accesso temporaneo a oggetti specifici. Per ulteriori informazioni, consulta Condivisione di oggetti con URL predefiniti nella Amazon S3 User Guide.

Il bucket Amazon S3 ha accesso pubblico in scrittura

I bucket Amazon S3 con accesso pubblico in scrittura consentono a chiunque su Internet di caricare, modificare o eliminare oggetti nel tuo bucket. Ciò comporta notevoli rischi per la sicurezza, tra cui la possibilità che qualcuno carichi file dannosi, modifichi file esistenti ed elimini dati. L'accesso pubblico in scrittura crea vulnerabilità di sicurezza che possono essere sfruttate dagli aggressori. Seguendo i principi di sicurezza standard, limita l'accesso in scrittura ai tuoi bucket Amazon S3 solo agli utenti e ai sistemi necessari.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Blocca l'accesso pubblico a livello di account e bucket

Amazon S3 fornisce impostazioni di accesso pubblico a blocchi che possono essere configurate sia a livello di bucket che di account per impedire l'accesso pubblico indipendentemente dalle policy

del bucket o dagli ACL. Per ulteriori informazioni, consulta Bloccare l'accesso pubblico allo storage Amazon S3 nella Amazon S3 User Guide.

Modifica le politiche dei bucket

Per un approccio più granulare alla rimozione dell'accesso pubblico in scrittura, consulta la policy del bucket. Puoi cercare`s3:PutObject`,`s3:DeleteObject`, o. `s3:*` Per ulteriori informazioni sulla gestione delle politiche dei bucket, consulta le politiche dei bucket per Amazon S3 nella Amazon S3 User Guide.

Metodi di accesso alternativi

Se è richiesto l'accesso pubblico in scrittura, considera queste alternative più sicure:

- URL prefirmati: utilizza gli URL prefirmati per l'accesso temporaneo a oggetti specifici. Per ulteriori informazioni, consulta Condivisione di oggetti con URL predefiniti nella Amazon S3 User Guide.
- Proxy Amazon API Gateway: utilizza un intermediario come API Gateway with AWS Lambda per convalidare e autorizzare le richieste prima di scrivere nel tuo bucket Amazon S3. Questo approccio garantisce che i clienti non scrivano mai direttamente nel bucket. Per ulteriori informazioni, consulta Tutorial: Create a REST API as a Amazon S3 proxy nella API Gateway Developer Guide.
- Amazon CloudFront: utilizzalo CloudFront con un Origin Access Control (OAC) configurato per firmare sempre le richieste. Abilita i metodi PUT e POST per consentire scritture autenticate senza esporre direttamente il bucket Amazon S3. Configura la tua policy sui bucket per limitare `s3:DeleteObject` le autorizzazioni solo ai principali autorizzati, in modo che gli utenti non autorizzati non possano eliminare gli oggetti che desideri conservare. Per ulteriori informazioni, consulta Limitare l'accesso a un'origine Amazon S3 nella Amazon Developer Guide. CloudFront

Caratteristiche dei dati sensibili per i bucket Amazon S3

Ecco le caratteristiche dei dati sensibili per i bucket Amazon S3 e le procedure di correzione suggerite.

Il bucket Amazon S3 contiene dati sensibili

Una scansione di sicurezza dei dati ha confermato la presenza di dati sensibili nel bucket Amazon S3. Un prodotto integrato per la sicurezza dei dati imposta questa caratteristica quando ispeziona gli oggetti nel bucket e identifica i contenuti che richiedono protezione. Security Hub riporta la caratteristica nello stesso modo indipendentemente dal prodotto che ha eseguito l'ispezione.

I dati sensibili possono includere:

- Credenziali
- Informazioni di identificazione personale
- Informazioni finanziarie
- Contenuti riservati che richiedono protezione

Se i dati sensibili vengono esposti a causa di una configurazione errata o di un accesso non autorizzato, potrebbero verificarsi violazioni della conformità, violazioni dei dati, furto di identità o perdite finanziarie. Seguendo le migliori pratiche di sicurezza, assicurati una corretta classificazione dei dati e il monitoraggio continuo dei dati sensibili nei tuoi bucket Amazon S3.

Correzione

Per eliminare questa caratteristica, rimuovi i dati sensibili dal bucket. Se il carico di lavoro richiede che il bucket memorizzi dati sensibili, implementa i seguenti controlli di sicurezza per ridurre il rischio di esposizione.

Esamina i dati sensibili nel bucket

Nella rilevazione dell'esposizione, scegli Open resource. Esamina il risultato sulla sicurezza dei dati che ha riportato i dati sensibili per determinare quali oggetti o prefissi li contengono. Se il rilevamento proviene da Macie, il tipo di risultato descrive la categoria di dati sensibili. Per ulteriori informazioni, consulta i risultati di Types of Macie nella Amazon Macie User Guide.

In base al tipo di dati sensibili rilevati, implementa i controlli di sicurezza appropriati:

- Limita l'accesso al bucket: rivedi le autorizzazioni del bucket per assicurarti che rispettino il principio del privilegio minimo. Usa le policy IAM, le politiche dei bucket e gli ACL per limitare l'accesso. Per ulteriori informazioni, consulta Identity and Access Management for Amazon S3 nella Amazon S3 User Guide.
- Abilita la crittografia lato server: abilita la crittografia lato server con chiavi KMS per una protezione aggiuntiva. Per ulteriori informazioni, consulta Using server-side encryption with AWS KMS keys () SSE-KMS nella Amazon S3 User Guide.
- Redazione o trasformazione dei dati sensibili: se gli oggetti non devono conservare valori sensibili, AWS Glue DataBrew utilizzali per preparare i dati. Applica le trasformazioni di mascheramento, sostituzione o hashing che rimuovono quei valori prima che i sistemi a valle consumino i dati. Scrivi

l'output preparato in un bucket separato con i propri controlli di accesso. Per ulteriori informazioni, consulta Che cos'è AWS Glue DataBrew? nella Guida per gli sviluppatori di AWS Glue DataBrew .

Correzione delle esposizioni per le istanze di notebook Amazon SageMaker

AWS Security Hub può generare risultati sull'esposizione per le istanze di SageMaker notebook Amazon.

Sulla console Security Hub, l'istanza del notebook coinvolta in un rilevamento dell'esposizione e le relative informazioni identificative sono elencate nella sezione Risorse dei dettagli del risultato. A livello di codice, è possibile recuperare i dettagli delle risorse con il GetFindingsV2funzionamento dell'API CSPM Security Hub.

Dopo aver identificato la risorsa coinvolta in un rilevamento dell'esposizione, puoi eliminare la risorsa se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per mitigare il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato sull'esposizione contiene i problemi identificati in diversi argomenti relativi alla correzione. Al contrario, è possibile risolvere un problema di esposizione e ridurne il livello di gravità affrontando un solo argomento di correzione. L'approccio alla risoluzione dei rischi dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida sulla correzione fornite in questo argomento potrebbero richiedere ulteriori consultazioni in altre risorse. AWS

Indice

- Caratteristiche di configurazione errate per le istanze di notebook Amazon SageMaker
  - L'istanza del SageMaker notebook Amazon ha l'accesso diretto a Internet abilitato
  - L'istanza del SageMaker notebook Amazon ha l'accesso root abilitato
- Caratteristiche dei dati sensibili per le istanze di SageMaker notebook Amazon
  - L'istanza Amazon SageMaker Notebook contiene dati sensibili
- Caratteristiche di impatto per le istanze di SageMaker notebook Amazon

- Dispone di un percorso di esecutore privilegiato con pieno controllo
- Ha un percorso diretto di escalation delle politiche
- Dispone di un percorso di dirottamento delle politiche di fiducia
- Ha un percorso di ransomware per i dati
- Ha un percorso di rimozione della restrizione
- Ha un percorso di creazione esecutore del ruolo
- Ha un percorso di esecuzione esistente di Swap Role
- Ha un percorso di escalation della catena di ruoli
- Dispone di un percorso di esecutore privilegiato per il codice di iniezione
- Ha disabilitato il percorso di audit trail
- Ha accesso al percorso dell'esecutore esistente
- Dispone di un percorso di coniazione delle credenziali
- Dispone di un percorso di accesso ai dati di accesso ai dati
- Ha un percorso di dirottamento del ruolo
- Dispone di un percorso di accesso ai dati a hop singolo
- Ha un percorso di avanzamento delle capacità
- Criticità aziendale

Caratteristiche di configurazione errate per le istanze di notebook Amazon SageMaker

Di seguito sono elencate le caratteristiche di errata configurazione delle istanze di SageMaker notebook Amazon e le procedure di correzione suggerite.

L'istanza del SageMaker notebook Amazon ha l'accesso diretto a Internet abilitato

Quando `DirectInternetAccess` è abilitato su un'istanza Amazon SageMaker Notebook, il traffico in uscita viene indirizzato a Internet attraverso un gateway NAT (SageMaker-managed Network Address Translation). Ciò fornisce un percorso di uscita che può essere utilizzato per l'esfiltrazione dei dati o come canale di comando e controllo se il notebook è compromesso. Seguendo le best practice di sicurezza, disabilita l'accesso diretto a Internet e posiziona le istanze dei notebook in un VPC con endpoint VPC per i servizi richiesti. AWS

Correzione

Intraprendi una o più delle seguenti azioni per ovviare a questa esposizione:

Disabilitare l'accesso a Internet diretto

L'`DirectInternetAccess`impostazione non può essere modificata dopo la creazione di un'istanza del notebook. Per disabilitarlo, crea una nuova istanza di notebook con `DirectInternetAccess` set to `Disabled` in una sottorete privata all'interno di un VPC, quindi migra i notebook e i dati dall'istanza esistente. Per istruzioni, consulta Connettere un'istanza di notebook in un VPC a risorse esterne nella Amazon SageMaker Developer Guide.

Configurare gli endpoint VPC

Quando l'accesso diretto a Internet è disabilitato, l'istanza notebook richiede endpoint VPC per accedere a AWS servizi come Amazon S3 e l'API Amazon. SageMaker Crea endpoint VPC di interfaccia per i servizi di cui ha bisogno il tuo notebook. Per informazioni sugli endpoint VPC, consulta Cos'è? AWS PrivateLink nella Guida.AWS PrivateLink

L'istanza del SageMaker notebook Amazon ha l'accesso root abilitato

Quando `RootAccess` è abilitato su un'istanza di SageMaker notebook Amazon, gli utenti dispongono dei privilegi di OS-level root completi. L'accesso root consente modifiche arbitrarie del sistema, backdoor persistenti e installazione di pacchetti senza restrizioni. Seguendo le migliori pratiche di sicurezza, disabilitate l'accesso root per le istanze dei notebook a meno che non sia esplicitamente richiesto per il flusso di lavoro.

Correzione: disabilita l'accesso root

Non è possibile modificare l'`RootAccess`impostazione su un'istanza di notebook in esecuzione. Per disabilitarla, arresta l'istanza, quindi aggiorna la configurazione dell'istanza `RootAccess` su`Disabled`. La maggior parte dei flussi di lavoro dei notebook, inclusa l'installazione di pacchetti con `pip` e l'esecuzione di configurazioni del ciclo di vita, continuano a funzionare senza accesso root. Per istruzioni, consulta Controllare l'accesso root a un'istanza di SageMaker notebook Amazon nella Amazon SageMaker Developer Guide.

Ulteriori considerazioni

Se è richiesto l'accesso root per attività specifiche, prendi in considerazione l'utilizzo dei notebook Amazon SageMaker Studio, che forniscono ambienti isolati basati su contenitori con controlli di accesso più granulari. Puoi anche utilizzare le configurazioni del ciclo di vita per preinstallare i pacchetti richiesti al momento della creazione dell'istanza, riducendo la necessità di accesso root durante il normale utilizzo.

Caratteristiche dei dati sensibili per le istanze di SageMaker notebook Amazon

Ecco le caratteristiche dei dati sensibili per le istanze di SageMaker notebook Amazon e le procedure di correzione suggerite.

L'istanza Amazon SageMaker Notebook contiene dati sensibili

Una scansione di sicurezza dei dati ha confermato che sull'istanza del SageMaker notebook Amazon sono presenti dati sensibili. Un prodotto integrato per la sicurezza dei dati definisce questa caratteristica. Il prodotto ispeziona i file, gli output e lo storage allegato del notebook e identifica i contenuti che richiedono protezione. Riportiamo questa caratteristica in Security Hub in modo coerente, indipendentemente dal prodotto integrato che ha eseguito l'ispezione.

I dati sensibili aumentano l'impatto di ogni altro punto debole sulla stessa istanza del notebook. Un ruolo di esecuzione permissivo, un percorso di uscita diretto da Internet o un accesso troppo ampio espone a contenuti regolamentati o riservati. Un aggressore che accede al notebook può leggere e copiare tali record dai file del notebook, dalle celle di output e dai checkpoint salvati. L'autore della minaccia può quindi conservare tali record al di fuori dell'ambiente dell'utente. Possono inoltre utilizzare qualsiasi credenziale trovata nel notebook per autenticarsi su altri sistemi.

Seguendo le procedure consigliate in materia di sicurezza, consigliamo di limitare l'accesso alle istanze dei notebook che contengono dati sensibili e di crittografare lo storage collegato quando è inattivo.

I dati sensibili possono includere:

- Credenziali, come password, chiavi di accesso e stringhe di connessione
- Informazioni di identificazione personale
- Informazioni finanziarie, come numeri di conto e dati delle carte di pagamento
- Contenuti riservati che richiedono protezione

La rimozione dei dati sensibili dal notebook è l'unico modo per eliminare questa caratteristica. Se il notebook deve fare riferimento a dati sensibili, le seguenti best practice di sicurezza riducono il rischio di esposizione.

Esamina i dati sensibili sull'istanza del notebook

Nel rilevamento dell'esposizione, apri la risorsa con il collegamento ipertestuale. Verrà aperta l'istanza del notebook interessata. Annota il nome dell'istanza del notebook, l' AWS account e la AWS

regione. Esamina i risultati sulla sicurezza dei dati che hanno riportato i dati sensibili per determinare quali file del notebook, celle di output o checkpoint li contengono.

In base al tipo di dati sensibili rilevati, implementa i controlli di sicurezza appropriati:

- Rimuovi i valori sensibili dal notebook: elimina i valori sensibili dal codice del notebook e cancella le celle di output che li contengono. Elimina tutti i checkpoint salvati e le copie esportate che conservano i valori. Se un valore deve rimanere referenziato, sostituiscilo con un segnaposto tokenizzato o mascherato. Per ulteriori informazioni, consulta Use Amazon SageMaker Notebook Instances nella Amazon SageMaker Developer Guide.
- Ruota le credenziali esposte: se il notebook conteneva credenziali, considerale compromesse. Disabilita e ruota le credenziali, quindi esamina i registri di controllo del sistema interessato per verificare l'utilizzo dei valori esposti. Recupera i segreti in fase di esecuzione AWS Secrets Manager utilizzando un ruolo di esecuzione con ambito ristretto anziché incorporarli nei contenuti del notebook. Per ulteriori informazioni, consulta Ruotare AWS Secrets Manager i segreti nella Guida per l'utente.AWS Secrets Manager
- Limita chi può aprire l'istanza del notebook: concedi l'accesso solo alle identità IAM che ne hanno bisogno. Ambita il ruolo di esecuzione in base alle azioni e alle risorse specifiche utilizzate dal notebook. Controlla chi può aprire il taccuino limitando le `sagemaker:CreatePresignedNotebookInstanceUrl` autorizzazioni. Per ulteriori informazioni, consulta gli esempi di policy SageMaker basate sull'identità di Amazon nella Amazon SageMaker Developer Guide.
- Crittografa lo spazio di archiviazione del notebook a riposo: collega una AWS KMS chiave all'istanza del notebook in modo che il volume di archiviazione che contiene i file e i checkpoint del notebook sia crittografato a riposo. Utilizza una chiave gestita dal cliente in modo da controllare la politica chiave. `kms:Decrypt`Concedi quella chiave solo alle identità che devono leggere il taccuino. Per ulteriori informazioni, consulta Proteggi i dati inattivi utilizzando la crittografia nell'Amazon SageMaker Developer Guide.
- Monitora l'accesso all'istanza del notebook: verifica AWS CloudTrail la `sagemaker:CreatePresignedNotebookInstanceUrl` presenza di chiamate e l'accesso da identità o fonti impreviste. Per ulteriori informazioni, consulta Registra le chiamate alle SageMaker API Amazon AWS CloudTrail nell'Amazon SageMaker Developer Guide.

Caratteristiche di impatto per le istanze di SageMaker notebook Amazon

Le caratteristiche di impatto descrivono il potenziale raggio di esplosione di un'esposizione. Security Hub analizza le autorizzazioni effettive del AWS Identity and Access Management principale

associato all'istanza del SageMaker notebook per determinare le risorse a valle che un utente malintenzionato potrebbe raggiungere se l'istanza del notebook viene compromessa, nonché la criticità aziendale di tali risorse. Ogni caratteristica di impatto identifica uno specifico modello di escalation dei privilegi. Per ridurre il raggio d'azione, esaminate i percorsi di autorizzazione descritti in ogni caratteristica e rimuovete eventuali privilegi non necessari.

Seguendo i principi di sicurezza standard, concedi il privilegio minimo fornendo solo le autorizzazioni necessarie per eseguire un'attività. Sostituisci politiche generali con politiche circoscritte che garantiscano solo le azioni e le risorse specifiche necessarie. Per identificare le autorizzazioni non utilizzate da rimuovere, utilizza IAM Access Analyzer per generare consigli basati sulla cronologia degli accessi. Per ulteriori informazioni, consulta Findings for external and inused access e Apply least-privilege permissions nella IAM User Guide.

Dispone di un percorso di esecutore privilegiato con pieno controllo

Il principale associato può passare un ruolo e inserire codice in una risorsa di calcolo che dispone già di autorizzazioni elevate. Ciò consente al principale di ottenere il pieno controllo sull'esecutore ed eseguire qualsiasi azione consentita dal ruolo dell'esecutore.

Ha un percorso diretto di escalation delle politiche

Il principale associato può modificare direttamente le politiche IAM per concedersi autorizzazioni aggiuntive, aumentando i propri privilegi senza risorse intermedie.

Dispone di un percorso di dirottamento delle politiche di fiducia

Il principale associato può modificare la politica di fiducia di un ruolo IAM per consentirsi di assumere quel ruolo, ottenendo le autorizzazioni del ruolo.

Ha un percorso di ransomware per i dati

Il principale associato può crittografare o eliminare i dati in un modo che potrebbe essere utilizzato per il ransomware, ad esempio crittografando gli oggetti Amazon S3 con una AWS KMS chiave gestita dal cliente e quindi modificando la politica della chiave.

Ha un percorso di rimozione della restrizione

Il principale associato può rimuovere le restrizioni di sicurezza come i limiti di autorizzazione, le politiche di controllo dei servizi o le dichiarazioni di rifiuto delle politiche basate sulle risorse, ampliando le funzionalità che possono fare gli altri principali o la risorsa stessa.

Ha un percorso di creazione esecutore del ruolo

Il principale associato può creare una nuova risorsa di calcolo (come una funzione Lambda o un'istanza Amazon EC2) e assegnarle un ruolo privilegiato, riciclando efficacemente le proprie autorizzazioni attraverso la nuova risorsa.

Ha un percorso di esecuzione esistente di Swap Role

Il principale associato può modificare il ruolo IAM associato a una risorsa di elaborazione esistente, sostituendolo con un ruolo più privilegiato per aumentare l'accesso.

Ha un percorso di escalation della catena di ruoli

Il principale associato può assumere una sequenza di ruoli, in cui ogni ruolo della catena dispone di autorizzazioni progressivamente più ampie, fino a raggiungere infine un ruolo altamente privilegiato.

Dispone di un percorso di esecutore privilegiato per il codice di iniezione

Il principale associato può iniettare codice in una risorsa di elaborazione in esecuzione che dispone di autorizzazioni elevate, eseguendo operazioni arbitrarie nell'ambito del ruolo privilegiato di tale risorsa.

Ha disabilitato il percorso di audit trail

Il responsabile associato può disabilitare i servizi di registrazione o monitoraggio CloudTrail, ad esempio coprire efficacemente le tracce durante o dopo un'escalation.

Ha accesso al percorso dell'esecutore esistente

Il principale associato può richiamare o connettersi a una risorsa di elaborazione esistente e utilizzare il ruolo associato per eseguire azioni privilegiate.

Dispone di un percorso di coniazione delle credenziali

Il principale associato può creare nuove credenziali a lungo termine (come chiavi di accesso o profili di accesso) per altri principali, stabilendo percorsi di accesso persistenti che sopravvivono alla rotazione delle password o alle scadenze delle sessioni.

Dispone di un percorso di accesso ai dati di accesso ai dati

Il responsabile associato può creare una risorsa di servizio e assegnarle un ruolo con accesso a dati sensibili, ottenendo l'accesso indiretto a tali dati tramite la nuova risorsa.

Ha un percorso di dirottamento del ruolo

Il principale associato può passare un ruolo a un'attività pianificata o basata su eventi (come una funzione Lambda attivata da un evento), consentendogli di eseguire codice arbitrario con le autorizzazioni di quel ruolo.

Dispone di un percorso di accesso ai dati a hop singolo

Il principale associato può accedere direttamente alle risorse di dati sensibili (come i bucket Amazon S3 o le tabelle DynamoDB) tramite le autorizzazioni esistenti, senza bisogno di passaggi di escalation intermedi.

Ha un percorso di avanzamento delle capacità

Il principale associato dispone di un percorso di assegnazione dei privilegi che ne migliora le capacità complessive oltre a quanto suggerirebbe l'assegnazione diretta delle autorizzazioni. Questa è una classificazione generale per i percorsi che non corrispondono a uno schema più specifico.

Criticità aziendale

La criticità aziendale della risorsa principale, stabilita dalle regole di automazione o dall'inferenza del nome e dei tag.

Correzione delle esposizioni per le macchine virtuali di Azure

AWS Security Hub può generare risultati sull'esposizione per le macchine virtuali di Azure.

Nella console di Security Hub, la macchina virtuale di Azure coinvolta nella rilevazione dell'esposizione e le relative informazioni identificative sono elencate nella sezione Risorse dei dettagli dei risultati. A livello di programmazione, è possibile recuperare i dettagli delle risorse con il GetFindingsV2 funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la correzione fornite in questo argomento potrebbero richiedere una consultazione aggiuntiva in altre risorse di Microsoft Azure.

Indice

- Tratti di configurazione errata per le macchine virtuali di Azure
  - La macchina virtuale di Azure dispone di un gruppo di sicurezza di rete aperto
  - La macchina virtuale di Azure ha una regola di sicurezza che consente l'accesso SSH o RDP
  - Al ruolo associato alla macchina virtuale di Azure è assegnato un ruolo di accesso amministrativo
  - La macchina virtuale di Azure ha un sistema operativo fuori uso
- Caratteristiche di raggiungibilità per le macchine virtuali di Azure
  - La macchina virtuale di Azure è raggiungibile tramite Internet
- Caratteristiche di vulnerabilità per le macchine virtuali di Azure
  - La macchina virtuale di Azure presenta vulnerabilità software sfruttabili in rete con un'alta probabilità di sfruttamento
  - La macchina virtuale di Azure presenta vulnerabilità software
  - La macchina virtuale di Azure contiene pacchetti software dannosi

Tratti di configurazione errata per le macchine virtuali di Azure

Ecco le caratteristiche di configurazione errata per le macchine virtuali di Azure e i passaggi di correzione suggeriti.

La macchina virtuale di Azure dispone di un gruppo di sicurezza di rete aperto

Un gruppo di sicurezza di rete (NSG) funge da firewall virtuale per la macchina virtuale di Azure, filtrando il traffico in entrata e in uscita con una serie di regole di sicurezza prioritarie. Un gruppo di sicurezza di rete aperto contiene regole che consentono l'accesso illimitato da qualsiasi fonte (ad esempio, una fonte di o). `Any` `0.0.0.0/0` Queste regole possono esporre la macchina virtuale ad accessi non autorizzati da Internet. Seguendo i principi di sicurezza standard, limita le regole del gruppo di sicurezza di rete solo agli indirizzi IP, alle porte e ai protocolli specifici richiesti dal carico di lavoro.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi le regole del gruppo di sicurezza di rete e valuta la configurazione corrente

Identifica il gruppo di sicurezza di rete associato all'interfaccia di rete o alla sottorete della macchina virtuale e rivedi le relative regole di sicurezza in entrata. Valuta quali porte consentono il traffico proveniente da ampi intervalli di sorgenti, come `Any` o. `0.0.0.0/0` Le regole vengono elaborate in ordine di priorità, quindi assicurati che una regola permissiva non abbia la precedenza su una più restrittiva. Per ulteriori informazioni, consulta Network security groups nella documentazione di Microsoft Azure.

Limita le regole dei gruppi di sicurezza di rete

Modifica o rimuovi le regole che consentono l'accesso senza restrizioni. Sostituisci un'ampia fonte, ad esempio `Any` con gli indirizzi IP affidabili specifici, gli intervalli CIDR, i tag di servizio o i gruppi di sicurezza delle applicazioni che richiedono l'accesso. Limita l'intervallo di porte di destinazione alle sole porte utilizzate dal carico di lavoro. Per ulteriori informazioni, vedi Gestire i gruppi di sicurezza di rete nella documentazione di Microsoft Azure.

La macchina virtuale di Azure ha una regola di sicurezza che consente l'accesso SSH o RDP

I protocolli di gestione remota come SSH (porta 22) e RDP (porta 3389) consentono agli utenti di connettersi e gestire macchine virtuali di Azure da postazioni remote. Quando una regola del gruppo di sicurezza di rete consente l'accesso a queste porte da Internet (una fonte di `Any` o`0.0.0.0/0`), la superficie di attacco della macchina virtuale aumenta in modo significativo ed è esposta ad attacchi di forza bruta e basati su credenziali. Seguendo i principi di sicurezza standard, limita l'accesso remoto a indirizzi IP specifici e affidabili o rimuovi completamente l'accesso diretto a Internet a queste porte.

Correzione

Intraprendi una o più delle seguenti azioni per ovviare a questa esposizione:

Limita la regola del gruppo di sicurezza di rete

Limita invece l'accesso SSH e RDP a specifici indirizzi IP o intervalli CIDR affidabili oppure rimuovi la regola in entrata se non è richiesto l'accesso remoto da Internet. `Any` Per ulteriori informazioni, vedi Gestire i gruppi di sicurezza di rete nella documentazione di Microsoft Azure.

Usa Azure Bastion per una connettività sicura

Invece di esporre le porte SSH o RDP a Internet, usa Azure Bastion per connetterti alla tua macchina virtuale tramite TLS senza un indirizzo IP pubblico o porte in entrata aperte. Per ulteriori informazioni, vedi Azure Bastion nella documentazione di Microsoft Azure.

Usa l'accesso istantaneo alla macchina virtuale

Abilita l'accesso alle macchine virtuali just-in-time (JIT) in Microsoft Defender for Cloud in modo che le porte di gestione come SSH e RDP rimangano chiuse per impostazione predefinita e aperte solo per le richieste approvate e limitate nel tempo provenienti da un indirizzo IP di origine specificato. Per ulteriori informazioni, consulta Abilitare l'accesso just-in-time nella documentazione di Microsoft Azure.

Al ruolo associato alla macchina virtuale di Azure è assegnato un ruolo di accesso amministrativo

Puoi assegnare un'identità gestita a una macchina virtuale di Azure e concederle assegnazioni di ruolo per il controllo degli accessi basato sui ruoli di Azure (Azure RBAC) per accedere ad altre risorse di Azure. Quando all'identità associata è assegnato un ruolo amministrativo (ad esempio `0wner` o`Contributor`) in un ambito ampio, in genere concede autorizzazioni ben oltre quelle richieste dal carico di lavoro. Se la macchina virtuale è compromessa, un utente malintenzionato può utilizzare queste autorizzazioni eccessive per spostarsi lateralmente nell'ambiente, accedere ai dati o manipolare le risorse. Seguendo i principi di sicurezza standard, concedi il privilegio minimo assegnando solo le autorizzazioni necessarie al carico di lavoro.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi e identifica le assegnazioni dei ruoli amministrativi

Nel portale di Azure, esamina le assegnazioni di ruolo per l'identità associata alla macchina virtuale. Cerca i ruoli di amministratore con privilegi`0wner`, ad esempio`Contributor`, o`User Access Administrator`, e i ruoli personalizzati che utilizzano un carattere jolly (`*`) nel loro. `Actions` Per ulteriori informazioni, consulta Elencare le assegnazioni di ruolo di Azure nella documentazione di Microsoft Azure.

Implementazione dell'accesso con privilegi minimi

Sostituisci le assegnazioni dei ruoli amministrativi con il ruolo integrato con il minor privilegio che concede solo le autorizzazioni richieste dal carico di lavoro. Assegnalo all'ambito più ristretto (risorsa

o gruppo di risorse) che soddisfa le tue esigenze. Quando crei ruoli personalizzati, specifica `Actions` e in `DataActions` modo esplicito invece di utilizzare un carattere jolly. Per ulteriori informazioni, vedi Best practice per Azure RBAC nella documentazione di Microsoft Azure.

La macchina virtuale di Azure ha un sistema operativo fuori uso

La macchina virtuale di Azure esegue un sistema operativo fuori uso che non è più supportato o gestito dal relativo fornitore. Quando un sistema operativo raggiunge la fine del ciclo di vita, il fornitore smette di rilasciare aggiornamenti e avvisi di sicurezza, il che lascia le vulnerabilità note permanentemente prive di patch ed espone la macchina virtuale agli attacchi. Seguendo le best practice di sicurezza, esegui l'upgrade a una versione del sistema operativo supportata.

Correzione: aggiornamento a una versione del sistema operativo supportata

Pianifica un aggiornamento sul posto o migra il carico di lavoro su una macchina virtuale che esegue una versione del sistema operativo supportata. Prima dell'aggiornamento, verifica la compatibilità dell'applicazione ed esegui un backup o un'istantanea in modo da poter eseguire il rollback se necessario. Per Windows, seguite le istruzioni per l'aggiornamento sul posto; per Linux, seguite le indicazioni all'aggiornamento fornite dal fornitore della distribuzione. Per ulteriori informazioni, vedi Eseguire un aggiornamento sul posto di una macchina virtuale Windows Server nella documentazione di Microsoft Azure.

Caratteristiche di raggiungibilità per le macchine virtuali di Azure

Ecco i tratti di raggiungibilità per le macchine virtuali di Azure e i passaggi di riparazione suggeriti.

La macchina virtuale di Azure è raggiungibile tramite Internet

Una macchina virtuale di Azure con porte raggiungibili da Internet potrebbe essere esposta ad attacchi. Una macchina virtuale diventa raggiungibile quando ha un indirizzo IP pubblico. Può anche diventare raggiungibile quando un sistema di bilanciamento del carico, un gateway applicativo o un altro percorso di rete consente il traffico in entrata da Internet. Seguendo i principi di sicurezza standard, implementa i controlli di accesso alla rete con privilegi minimi limitando il traffico in entrata solo alle fonti e alle porte necessarie.

Correzione

Intraprendi una o più delle seguenti azioni per ovviare a questa esposizione:

Limita o rimuovi l'esposizione a Internet

Verifica se la macchina virtuale richiede un indirizzo IP pubblico. In caso contrario, dissocia l'indirizzo IP pubblico dall'interfaccia di rete e utilizza invece un indirizzo IP privato. Se è ancora necessaria la connettività Internet in uscita, utilizza un gateway NAT.

Se è richiesto l'accesso in entrata, posiziona la macchina virtuale dietro un load balancer, Azure Firewall o un application gateway anziché esporla direttamente. Per ulteriori informazioni, vedi Indirizzi IP pubblici nella documentazione di Microsoft Azure.

Rafforzare le regole dei gruppi di sicurezza della rete in entrata

Modifica o rimuovi le regole del gruppo di sicurezza della rete in entrata che consentono l'accesso illimitato (Anyo`0.0.0.0/0`) e limita l'accesso agli intervalli di sorgenti, alle porte e ai protocolli specifici richiesti dal carico di lavoro. Per ulteriori informazioni, vedi Network security groups nella documentazione di Microsoft Azure.

Usa Azure Bastion per l'accesso alla gestione

Per la connettività di gestione, usa Azure Bastion per raggiungere la macchina virtuale tramite TLS senza un indirizzo IP pubblico o porte aperte. SSH/RDP Per ulteriori informazioni, vedi Azure Bastion nella documentazione di Microsoft Azure.

Caratteristiche di vulnerabilità per le macchine virtuali di Azure

Ecco le caratteristiche di vulnerabilità per le macchine virtuali di Azure e i passaggi di correzione suggeriti.

La macchina virtuale di Azure presenta vulnerabilità software sfruttabili in rete con un'alta probabilità di sfruttamento

Le vulnerabilità e le esposizioni comuni (CVE) possono influire sui pacchetti software installati nelle macchine virtuali di Azure. Una vulnerabilità ad alta priorità è sfruttabile in rete con un'alta probabilità di sfruttamento. Ciò rappresenta una minaccia immediata alla sicurezza perché il codice di exploit potrebbe essere già disponibile al pubblico e utilizzato attivamente dagli aggressori o dagli strumenti di scansione automatici. Correggi tempestivamente queste vulnerabilità per proteggere la tua macchina virtuale.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi e correggi il risultato

Usa la valutazione delle vulnerabilità di Microsoft Defender for Cloud per esaminare i CVE interessati e le fasi di riparazione per la macchina virtuale. Il riquadro dei dettagli di ogni risultato include i CVE pertinenti e le soluzioni correttive consigliate. Per ulteriori informazioni, vedi Correggere le vulnerabilità dei computer nella documentazione di Microsoft Azure.

Applica gli aggiornamenti

Usa Azure Update Manager per valutare e distribuire gli aggiornamenti del sistema operativo e del software nelle tue macchine virtuali in base a una pianificazione. Se un aggiornamento non è disponibile, valuta la possibilità di rimuovere o disabilitare il software vulnerabile o di limitarne l'accesso alla rete, fino al rilascio di una patch. Per ulteriori informazioni, vedi Azure Update Manager nella documentazione di Microsoft Azure.

Considerazioni future

Per evitare che si verifichino in futuro, consenti a Microsoft Defender for Servers di scansionare continuamente le tue macchine virtuali alla ricerca di vulnerabilità e di stabilire una pianificazione regolare per l'applicazione delle patch con Azure Update Manager. Per ulteriori informazioni, consulta Microsoft Defender for Servers nella documentazione di Microsoft Azure.

La macchina virtuale di Azure presenta vulnerabilità software

Le vulnerabilità e le esposizioni comuni (CVE) possono influire sui pacchetti software installati nelle macchine virtuali di Azure. Le vulnerabilità non critiche rappresentano punti deboli di sicurezza con gravità o sfruttabilità inferiori rispetto alle vulnerabilità ad alta priorità. Sebbene rappresentino un rischio meno immediato, gli aggressori possono comunque sfruttare le vulnerabilità prive di patch per compromettere la riservatezza, l'integrità o la disponibilità dei dati o per accedere ad altri sistemi. Seguendo le best practice di sicurezza, correggi queste vulnerabilità per proteggere la tua macchina virtuale dagli attacchi.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi e correggi il risultato

Usa la valutazione delle vulnerabilità di Microsoft Defender for Cloud per esaminare i CVE interessati e seguire i passaggi di correzione nel riquadro dei dettagli dei risultati. Per ulteriori informazioni, consulta Risolvere le vulnerabilità dei computer nella documentazione di Microsoft Azure.

Applica gli aggiornamenti

Usa Azure Update Manager per valutare e distribuire gli aggiornamenti del sistema operativo e del software nelle tue macchine virtuali. Per gestire gli aggiornamenti in modo coerente su larga scala, configura le patch pianificate. Per ulteriori informazioni, vedi Azure Update Manager nella documentazione di Microsoft Azure.

La macchina virtuale di Azure contiene pacchetti software dannosi

I pacchetti dannosi sono componenti software che contengono codice dannoso progettato per compromettere la riservatezza, l'integrità e la disponibilità dei sistemi e dei dati. I pacchetti dannosi rappresentano una minaccia attiva e critica per la macchina virtuale, poiché gli aggressori possono eseguire il codice dannoso automaticamente senza sfruttare una vulnerabilità separata. Seguendo le best practice di sicurezza, rimuovi i pacchetti dannosi per proteggere la tua macchina virtuale da potenziali attacchi.

Soluzione: analizza e rimuovi i pacchetti dannosi

Esamina i dettagli dei risultati per comprendere la minaccia e identificare i pacchetti interessati, quindi rimuovi i pacchetti identificati utilizzando il gestore di pacchetti appropriato per il sistema operativo. Dopo la rimozione, esegui una scansione per confermare che non rimangano componenti dannosi correlati. Per ulteriori informazioni, vedi Microsoft Defender for Servers nella documentazione di Microsoft Azure.

Correzione delle esposizioni per i contenitori BLOB di Azure Storage

AWS Security Hub può generare risultati di esposizione per i contenitori BLOB di Azure Storage.

Nella console di Security Hub, il contenitore blob di Azure Storage coinvolto nel rilevamento dell'esposizione e le relative informazioni identificative sono elencati nella sezione Risorse dei dettagli dei risultati. A livello di programmazione, è possibile recuperare i dettagli delle risorse con il GetFindingsV2 funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la correzione fornite in questo argomento potrebbero richiedere una consultazione aggiuntiva in altre risorse di Microsoft Azure.

Indice

- Caratteristiche di raggiungibilità per i contenitori blob di Azure Storage
  - L'account di archiviazione consente l'accesso anonimo ai blob
- Caratteristiche di errata configurazione per i contenitori blob di Azure Storage
  - L'account di archiviazione non richiede HTTPS per le operazioni di trasferimento
  - L'account di archiviazione non è crittografato con chiavi gestite dal cliente
  - L'account di archiviazione consente l'accesso tra tenant
  - L'eliminazione automatica dei blob è disattivata nell'account di archiviazione
  - L'account di archiviazione consente l'eliminazione permanente dei blob eliminati automaticamente
  - Il contenitore blob di Azure Storage ha il controllo delle versioni dei blob disabilitato
  - Il contenitore di archiviazione non ha una politica di immutabilità

Caratteristiche di raggiungibilità per i contenitori blob di Azure Storage

Ecco le caratteristiche di raggiungibilità per i contenitori blob di Azure Storage e i passaggi di riparazione suggeriti.

L'account di archiviazione consente l'accesso anonimo ai blob

Quando l'accesso in lettura anonimo è abilitato, i client non autenticati possono leggere i dati BLOB senza autorizzazione. Quando l'account di archiviazione consente l'accesso anonimo (pubblico) ai blob e il livello di accesso di un contenitore lo consente, chiunque su Internet pubblico può leggere i dati in quel contenitore. Seguendo i principi di sicurezza standard, impedite l'accesso anonimo a livello di account e richiedete l'autorizzazione di ogni richiesta, a meno che lo scenario non dipenda esplicitamente dall'accesso pubblico in lettura.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Disabilita l'accesso anonimo per l'account di archiviazione

Imposta la `AllowBlobPublicAccess` proprietà dell'account di archiviazione su`false`. La disattivazione dell'accesso anonimo a livello di account ha la precedenza sulle impostazioni di accesso di tutti i contenitori dell'account e blocca le future richieste anonime. Per ulteriori informazioni, vedi Impedire l'accesso in lettura anonimo nella documentazione di Microsoft Azure.

Imposta il livello di accesso al contenitore su privato

Se i singoli contenitori sono stati configurati per l'accesso pubblico, imposta il livello di accesso anonimo di ciascun contenitore `Private` in modo che tutte le richieste richiedano l'autorizzazione. Prima di modificare l'impostazione, esaminate tutte le applicazioni client che potrebbero dipendere dall'accesso anonimo. Per ulteriori informazioni, vedi Configurare l'accesso in lettura anonimo nella documentazione di Microsoft Azure.

Caratteristiche di errata configurazione per i contenitori blob di Azure Storage

Ecco le caratteristiche di configurazione errata per i contenitori blob di Azure Storage e i passaggi di correzione suggeriti.

L'account di archiviazione non richiede HTTPS per le operazioni di trasferimento

Quando un account di archiviazione non richiede un trasferimento sicuro, accetta richieste tramite HTTP non crittografato. I dati e le credenziali inviati tramite HTTP possono essere intercettati o modificati in transito da un utente malintenzionato sul percorso di rete. Seguendo i principi di sicurezza standard, richiedi un trasferimento sicuro in modo che l'account accetti richieste solo tramite HTTPS.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Richiedi un trasferimento sicuro

Abilita la proprietà Secure transfer required sull'account di archiviazione (la `enableHttpsTrafficOnly` proprietà). Quando è richiesto un trasferimento sicuro, qualsiasi richiesta effettuata tramite HTTP viene rifiutata. Per ulteriori informazioni, vedi Require secure transfer nella documentazione di Microsoft Azure.

Applica una versione TLS minima

Imposta la versione TLS minima dell'account di archiviazione su 1.2 (la `minimumTlsVersion` proprietà) in modo che le richieste che utilizzano versioni del protocollo precedenti e meno sicure vengano rifiutate. Verifica che i tuoi client supportino TLS 1.2 prima di applicare questa impostazione. Per ulteriori informazioni, vedi Configurare la versione TLS minima per un account di archiviazione nella documentazione di Microsoft Azure.

L'account di archiviazione non è crittografato con chiavi gestite dal cliente

Per impostazione predefinita, Azure Storage crittografa i dati inattivi con chiavi. Microsoft-managed Customer-managed le chiavi (CMK) ti danno il controllo sulla chiave che protegge i tuoi dati, inclusa la possibilità di ruotare, revocare e controllare l'accesso alla chiave. Se i requisiti di conformità della tua organizzazione richiedono il controllo sulle chiavi di crittografia, l'assenza di chiavi gestite dal cliente è una lacuna. Seguendo le best practice per la protezione dei dati, configura l'account di archiviazione per utilizzare le chiavi gestite dal cliente archiviate in Azure Key Vault o in un HSM gestito.

Correzione: configura le chiavi gestite dal cliente

Archivia una chiave in Azure Key Vault o Azure Key Vault Managed HSM, con la protezione da eliminazione graduale ed eliminazione abilitata. Concedi a un'identità gestita il`get`, e le `unwrapkey` autorizzazioni`wrapkey`, quindi configura l'account di archiviazione per utilizzare quella chiave per la crittografia. È possibile passare dalla modalità gestita dal cliente a quella con Microsoft-managed chiavi in qualsiasi momento. Per ulteriori informazioni, vedi Customer-managed Keys for Storage Encryption nella documentazione di Microsoft Azure.

L'account di archiviazione consente l'accesso tra tenant

Cross-tenant le impostazioni di accesso, ad esempio la replica di oggetti tra tenant o la delega SAS (Shared Access Signature) tra più tenant, possono far sì che i dati lascino il tenant Microsoft Entra proprietario dell'account di archiviazione. Se il carico di lavoro non richiede la condivisione dei dati tra tenant, lasciare attive queste impostazioni aumenta il rischio che i dati escano dai confini del tenant. Seguendo i principi di sicurezza standard, disabilita l'accesso tra tenant a meno che non sia esplicitamente richiesto.

Soluzione: disabilita le impostazioni di accesso tra tenant

Sull'account di storage, disabilita la replica di oggetti tra tenant (impostata su`false`) e, se supportata, limita la `allowCrossTenantReplication` delega SAS tra tenant. Rivedi i requisiti di replica e condivisione prima di apportare la modifica. Per ulteriori informazioni, consulta la panoramica dell'account Azure Storage nella documentazione di Microsoft Azure.

L'eliminazione automatica dei blob è disattivata nell'account di archiviazione

Blob soft delete protegge singoli BLOB, istantanee e versioni dall'eliminazione e dalla sovrascrittura accidentali o dolose. Conserva i dati eliminati per un periodo di conservazione configurabile, durante il quale è possibile ripristinarli. Quando l'eliminazione automatica è disattivata, i dati BLOB eliminati o sovrascritti non possono essere ripristinati, il che espone l'account a una perdita permanente di dati. Seguendo le best practice per la protezione dei dati, abilita la soft delete dei blob con un periodo di conservazione appropriato.

Soluzione: abilita l'eliminazione graduale dei blob

Abilita l'eliminazione graduale dei blob sull'account di archiviazione e imposta un periodo di conservazione (da 1 a 365 giorni) che soddisfi i requisiti di ripristino. Per una protezione più completa, abilita anche il soft delete dei contenitori e il controllo delle versioni dei blob. Per ulteriori informazioni, vedi Soft delete for blob nella documentazione di Microsoft Azure.

L'account di archiviazione consente l'eliminazione permanente dei blob eliminati automaticamente

Quando l'eliminazione permanente è consentita (la `allowPermanentDelete` proprietà è`true`), i blob e le istantanee eliminati temporaneamente possono essere rimossi prima della scadenza del periodo di conservazione dell'eliminazione automatica. Ciò compromette la protezione fornita dall'eliminazione graduale, in quanto un utente o un responsabile compromesso può distruggere definitivamente i dati recuperabili prima della scadenza del periodo di conservazione. Seguendo le best practice per la protezione dei dati, non consentite l'eliminazione permanente dei blob eliminati automaticamente a meno che non abbiate un requisito specifico e ben compreso.

Soluzione: disabilita l'eliminazione permanente

Imposta la `allowPermanentDelete` proprietà dell'account di archiviazione `false` in modo che i BLOB e le istantanee eliminati automaticamente rimangano recuperabili per l'intero periodo di conservazione. Per ulteriori informazioni, vedi Soft delete for blob nella documentazione di Microsoft Azure.

Il contenitore blob di Azure Storage ha il controllo delle versioni dei blob disabilitato

Il controllo delle versioni dei blob mantiene automaticamente le versioni precedenti di un blob. Quando un blob viene modificato o eliminato, lo stato precedente viene mantenuto come versione precedente che è possibile ripristinare. Quando il controllo delle versioni è disabilitato, le sovrascritture e le eliminazioni non possono essere ripristinate a uno stato precedente, il che

aumenta il rischio di perdita o danneggiamento irreversibile dei dati. Seguendo le best practice di protezione dei dati, abilita il controllo delle versioni dei blob, insieme alla cancellazione automatica, per una protezione ottimale dei dati.

Correzione: abilita il controllo delle versioni dei blob

Abilita il controllo delle versioni sul servizio BLOB dell'account di archiviazione. Per controllare il costo della conservazione di molte versioni, utilizza una politica di gestione del ciclo di vita per eliminare automaticamente le vecchie versioni. Per ulteriori informazioni, consulta Blob versioning nella documentazione di Microsoft Azure.

Il contenitore di archiviazione non ha una politica di immutabilità

Una politica di immutabilità memorizza i dati BLOB in uno stato WORM (Write Once, Read Many). In questo stato, i dati non possono essere modificati o eliminati per un intervallo specificato (una politica di conservazione basata sul tempo) o fino a quando non viene cancellata una conservazione legale. Senza una politica di immutabilità, i dati aziendali critici o rilevanti per la conformità contenuti nel contenitore possono essere sovrascritti o eliminati, anche da utenti privilegiati. Laddove si applichino requisiti normativi o di integrità dei dati, configura una politica di immutabilità per il contenitore.

Correzione: configura una politica di immutabilità

Configura una politica di conservazione basata sul tempo o una conservazione legale del contenitore. Blocca la politica basata sul tempo una volta completato il test in modo che i dati siano completamente protetti in uno stato WORM. Abilita l'eliminazione graduale prima di applicare le politiche di immutabilità per una protezione aggiuntiva. Per ulteriori informazioni, vedi Archiviazione immutabile per dati BLOB nella documentazione di Microsoft Azure.

Correzione delle esposizioni per i database SQL di Azure

AWS Security Hub può generare risultati di esposizione per i database SQL di Azure.

Nella console Security Hub, il database SQL di Azure coinvolto nella ricerca dell'esposizione e le relative informazioni identificative sono elencati nella sezione Risorse dei dettagli dei risultati. A livello di programmazione, è possibile recuperare i dettagli delle risorse con il GetFindingsV2 funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i

costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la correzione fornite in questo argomento potrebbero richiedere una consultazione aggiuntiva in altre risorse di Microsoft Azure.

Indice

- Caratteristiche di configurazione errata per i database SQL di Azure
  - Nel database SQL di Azure è abilitato l'accesso alla rete pubblica
  - Il database SQL di Azure non impone l'autenticazione di Azure AD-only
  - Il database SQL di Azure utilizza un nome utente amministratore predefinito o comune
  - Il backup geo-ridondante è disabilitato nel database SQL di Azure

Caratteristiche di configurazione errata per i database SQL di Azure

Ecco le caratteristiche di errata configurazione per i database SQL di Azure e i passaggi di correzione suggeriti.

Nel database SQL di Azure è abilitato l'accesso alla rete pubblica

Quando l'accesso alla rete pubblica è abilitato sul server logico, il database è raggiungibile tramite un endpoint pubblico e può accettare connessioni dalla rete Internet pubblica (soggette alle regole del firewall). Un endpoint pubblico aumenta la superficie di attacco del database e lo espone a tentativi di connessione non autorizzati. Seguendo i principi di sicurezza standard, disabilita l'accesso alla rete pubblica e connettiti al database privatamente, oppure limita rigorosamente le regole del firewall del server.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Disabilita l'accesso alla rete pubblica e utilizza Private Link

Imposta l'accesso alla rete pubblica del server logico `Disabled` e connettiti al database tramite un endpoint privato (Azure Private Link) all'interno della tua rete virtuale. In questo modo il traffico del database viene mantenuto sulla dorsale di Azure e lontano dalla rete Internet pubblica. Per ulteriori informazioni, vedi Controlli di accesso alla rete per il database SQL di Azure nella documentazione di Microsoft Azure.

Limita le regole del firewall se è richiesto l'accesso pubblico

Se devi mantenere abilitato l'accesso pubblico, rimuovi qualsiasi regola che consenta l'accesso a Internet completo e disabilita Consenti ai servizi e alle risorse di Azure di accedere a questo server quando non è necessario. Limita le regole del firewall a livello di server agli indirizzi IP attendibili specifici richiesti dal carico di lavoro. Per ulteriori informazioni, vedi Controlli dell'accesso alla rete per il database SQL di Azure nella documentazione di Microsoft Azure.

Applica una versione TLS minima

Imposta la versione TLS minima del server logico su 1.2 in modo che le connessioni che utilizzano versioni di protocollo precedenti e meno sicure vengano rifiutate. Verifica che i tuoi client supportino TLS 1.2 prima di applicare questa impostazione. Per ulteriori informazioni, vedi Impostazioni di connettività per il database SQL di Azure nella documentazione di Microsoft Azure.

Il database SQL di Azure non impone l'autenticazione di Azure AD-only

Quando Entra-only l'autenticazione Microsoft (in precedenza AD-only autenticazione di Azure) non viene applicata, il server logico accetta anche l'autenticazione SQL, che si basa su password archiviate e gestite all'interno del database. L'autenticazione SQL è più suscettibile al furto di credenziali e agli attacchi di forza bruta e non trae vantaggio dai controlli centralizzati di Microsoft Entra come l'accesso condizionale e l'autenticazione a più fattori. Seguendo i principi di sicurezza standard, applica l' Entra-only autenticazione Microsoft in modo che solo le identità Microsoft Entra possano connettersi.

Soluzione: applica l'autenticazione Microsoft Entra-only

Imposta un amministratore Microsoft Entra per il server logico, quindi abilita l'autenticazione Microsoft Entra-only . Ciò disabilita l'autenticazione SQL in modo che solo le identità Microsoft Entra possano connettersi al server e ai relativi database. Verifica che le tue applicazioni supportino l'autenticazione Microsoft Entra prima di applicare questa impostazione. Per ulteriori informazioni, consulta Entra-only l'autenticazione Microsoft nella documentazione di Microsoft Azure.

Il database SQL di Azure utilizza un nome utente amministratore predefinito o comune

L'accesso dell'amministratore del server logico utilizza un nome utente noto o comune, ad esempio `sqladminadmin`, `osa`. I nomi utente degli amministratori più comuni sono prevedibili, il che rende il server un bersaglio più facile per attacchi di forza bruta e furto di credenziali, in quanto un utente malintenzionato deve solo indovinare la password. Seguendo i principi di sicurezza standard, evita i nomi utente di amministratore predefiniti o comuni e centralizza l'accesso amministrativo tramite Microsoft Entra ID.

Soluzione: utilizzare un amministratore non predefinito e l'autenticazione Microsoft Entra

Evita nomi di accesso amministrativi prevedibili. Ove possibile, applica Entra-only l'autenticazione Microsoft e gestisci l'accesso amministrativo tramite identità e gruppi Microsoft Entra anziché un accesso da amministratore SQL. Segui le best practice di sicurezza di Azure SQL per la gestione degli accessi e degli accessi con privilegi minimi. Per ulteriori informazioni, consulta le best practice di sicurezza del database SQL di Azure nella documentazione di Microsoft Azure.

Il backup geo-ridondante è disabilitato nel database SQL di Azure

Per impostazione predefinita, il database SQL di Azure archivia i backup automatici in uno spazio di archiviazione georidondante, che replica i backup in un'area associata e consente il ripristino geografico durante un'interruzione regionale. Quando la ridondanza dello storage di backup è invece impostata su storage ridondante localmente o ridondante per zona, il ripristino geografico non è disponibile. Non è possibile ripristinare il database in un'altra regione se la regione principale non è disponibile. Seguendo le best practice di protezione dei dati, utilizza uno storage di backup georidondante per i database che richiedono resilienza alle interruzioni regionali.

Correzione

Intraprendi una o più delle seguenti azioni per ovviare a questa esposizione:

Configura lo storage di backup geo-ridondante

Imposta la ridondanza dello storage di backup del database su geo-redundant storage (GRS) o geo-zone-redundant storage (GZRS) in modo che il ripristino geografico sia disponibile. Le modifiche si applicano ai backup futuri e possono richiedere fino a 48 ore per avere effetto. Per ulteriori informazioni, vedi Backup automatici nel database SQL di Azure nella documentazione di Microsoft Azure.

Configurare la conservazione a lungo termine

Per i database con requisiti di conformità o ripristino a lungo termine, configura una politica di conservazione a lungo termine (LTR). LTR conserva i backup completi per un massimo di 10 anni, oltre alla conservazione a breve termine predefinita. Per ulteriori informazioni, vedi Long-term Conservazione nel database SQL di Azure nella documentazione di Microsoft Azure.

Correzione delle esposizioni per gli account Azure Cosmos DB

AWS Security Hub può generare risultati di esposizione per gli account Azure Cosmos DB.

Nella console Security Hub, l'account Azure Cosmos DB coinvolto nella rilevazione dell'esposizione e le relative informazioni identificative sono elencati nella sezione Risorse dei dettagli dei risultati. A livello di programmazione, puoi recuperare i dettagli delle risorse con il GetFindingsV2 funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la correzione fornite in questo argomento potrebbero richiedere una consultazione aggiuntiva in altre risorse di Microsoft Azure.

Indice

- Caratteristiche di configurazione errata per gli account Azure Cosmos DB
  - L'account Azure Cosmos DB ha l'accesso alla rete pubblica abilitato
  - L'account Azure Cosmos DB non utilizza il backup continuo

Caratteristiche di configurazione errata per gli account Azure Cosmos DB

Ecco le caratteristiche di configurazione errata per gli account Azure Cosmos DB e i passaggi di correzione suggeriti.

L'account Azure Cosmos DB ha l'accesso alla rete pubblica abilitato

Quando l'accesso alla rete pubblica è abilitato, l'account Azure Cosmos DB è raggiungibile tramite un endpoint pubblico. Può accettare connessioni dalla rete Internet pubblica, soggette alle regole del firewall e della rete virtuale. Un endpoint pubblico aumenta la superficie di attacco del tuo account e lo espone a tentativi di connessione non autorizzati e a potenziali esfiltrazioni di dati. Seguendo i principi di sicurezza standard, disabilita l'accesso alla rete pubblica e connettiti all'account privatamente, oppure limita rigorosamente le regole del firewall dell'account.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Disabilita l'accesso alla rete pubblica e utilizza Private Link

Imposta la `publicNetworkAccess` proprietà dell'account `Disabled` e connettiti tramite un endpoint privato (Azure Private Link) all'interno della tua rete virtuale. Se combinati con politiche restrittive di gruppo di sicurezza di rete, gli endpoint privati aiutano a ridurre il rischio di esfiltrazione dei dati. Per ulteriori informazioni, vedi Configurare Azure Private Link nella documentazione di Microsoft Azure.

Limita le regole del firewall se è richiesto l'accesso pubblico

Se devi mantenere abilitato l'accesso pubblico, configura le regole del firewall IP e le regole della rete virtuale in modo da consentire solo le specifiche fonti attendibili richieste dal tuo carico di lavoro, invece di consentire tutte le reti. Per ulteriori informazioni, vedi Configurare il firewall IP nella documentazione di Microsoft Azure.

L'account Azure Cosmos DB non utilizza il backup continuo

Con la modalità di backup continuo, puoi utilizzare il ripristino point-in-time per eseguire il ripristino da una scrittura o un'eliminazione accidentale. Puoi anche ripristinare un database o un contenitore eliminato con qualsiasi timestamp entro il periodo di conservazione. Quando l'account utilizza la modalità di backup periodico anziché il backup continuo, non è possibile eseguire il ripristino point-in-time self-service. Questa limitazione aumenta i tempi di ripristino e il rischio di perdita dei dati dopo una modifica accidentale o dolosa. Seguendo le best practice per la protezione dei dati, abilita la modalità di backup continuo laddove il carico di lavoro la supporti.

Soluzione: attiva la modalità di backup continuo

Configura l'account per utilizzare la modalità di backup continuo (livello di 7 o 30 giorni) in modo che sia disponibile il ripristino point-in-time. Rivedi le limitazioni attuali e le API supportate prima di

migrare dal backup periodico a quello continuo. Per ulteriori informazioni, vedi Backup continuo con ripristino point-in-time nella documentazione di Microsoft Azure.

Correzione delle esposizioni per le app Azure Function

AWS Security Hub può generare risultati sull'esposizione per le app Azure Function.

Nella console Security Hub, l'app Azure Function coinvolta nella rilevazione dell'esposizione e le relative informazioni identificative sono elencate nella sezione Risorse dei dettagli dei risultati. A livello di programmazione, è possibile recuperare i dettagli delle risorse con il GetFindingsV2 funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la correzione fornite in questo argomento potrebbero richiedere una consultazione aggiuntiva in altre risorse di Microsoft Azure.

Indice

- Caratteristiche di configurazione errata per le app Azure Function
  - L'app Azure Function è distribuita all'esterno di una rete virtuale
  - Al ruolo associato all'app Azure Function è assegnato un ruolo di accesso amministrativo
- Caratteristiche di raggiungibilità per le app Azure Function
  - L'app Azure Function consente l'invocazione anonima del trigger HTTP
- Caratteristiche di vulnerabilità per le app Azure Function
  - L'app Azure Function presenta vulnerabilità software sfruttabili in rete con un'alta probabilità di sfruttamento

- L'app Azure Function presenta vulnerabilità software
- L'app Azure Function contiene pacchetti software dannosi

Caratteristiche di configurazione errata per le app Azure Function

Ecco le caratteristiche di configurazione errata per le app Azure Function e i passaggi di correzione suggeriti.

L'app Azure Function è distribuita all'esterno di una rete virtuale

Quando un'app Function non è integrata con una rete virtuale, i relativi endpoint e il traffico in uscita attraversano la rete pubblica anziché i confini della rete privata. Quando l'app Function non è integrata con una rete virtuale, non è possibile applicare controlli a livello di rete come endpoint privati, gruppi di sicurezza di rete e accesso limitato in uscita. Questa lacuna aumenta l'esposizione dell'app. Seguendo i principi di sicurezza standard, integra l'app Function con una rete virtuale e utilizza endpoint privati laddove il tuo piano di hosting la supporti.

Correzione

Intraprendi una o più delle seguenti azioni per affrontare questa esposizione:

Integra l'app Function con una rete virtuale

Abilita l'integrazione della rete virtuale per l'app Function. Se supportato dal tuo piano di hosting (Flex Consumption, Elastic Premium o Dedicated), utilizza endpoint privati in modo che l'app sia raggiungibile solo dall'interno della tua rete. Per ulteriori informazioni, consulta le opzioni di rete di Azure Functions nella documentazione di Microsoft Azure.

Limita l'accesso in entrata

Nei piani di hosting che non supportano gli endpoint privati, utilizza le restrizioni di accesso per consentire il traffico in entrata solo da intervalli di indirizzi IP affidabili e disabilita l'accesso alla rete pubblica laddove non sia richiesto. Per ulteriori informazioni, consulta Impostare le restrizioni di accesso nella documentazione di Microsoft Azure.

Al ruolo associato all'app Azure Function è assegnato un ruolo di accesso amministrativo

Puoi assegnare un'identità gestita a un'app Azure Function e concederle assegnazioni di ruolo per il controllo degli accessi basato sui ruoli di Azure (Azure RBAC) per accedere ad altre risorse

di Azure. Quando l'identità associata ha un'assegnazione di ruolo amministrativo (ad esempio `0wner` o`Contributor`) in un ambito ampio, in genere concede autorizzazioni ben oltre quelle richieste dall'app. Se l'app Function è compromessa, un utente malintenzionato può utilizzare queste autorizzazioni eccessive per spostarsi lateralmente nell'ambiente, accedere ai dati o manipolare le risorse. Seguendo i principi di sicurezza standard, concedi il privilegio minimo assegnando solo le autorizzazioni necessarie all'app.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi e identifica le assegnazioni dei ruoli amministrativi

Nel portale di Azure, esamina le assegnazioni di ruolo per l'identità associata all'app Function. Cerca i ruoli di amministratore con privilegi`0wner`, come`Contributor`, o`User Access Administrator`, e i ruoli personalizzati che utilizzano un carattere jolly (`*`) nel loro. `Actions` Per ulteriori informazioni, consulta Elencare le assegnazioni di ruolo di Azure nella documentazione di Microsoft Azure.

Implementazione dell'accesso con privilegi minimi

Sostituisci le assegnazioni dei ruoli amministrativi con il ruolo predefinito con il minor privilegio che concede solo le autorizzazioni richieste dall'app e assegnalo nell'ambito più ristretto che soddisfa le tue esigenze. Usa un'identità gestita anziché i segreti archiviati per le connessioni ad altri servizi di Azure. Per ulteriori informazioni, vedi Best practice per Azure RBAC nella documentazione di Microsoft Azure.

Caratteristiche di raggiungibilità per le app Azure Function

Ecco le caratteristiche di raggiungibilità per le app Azure Function e i passaggi di correzione suggeriti.

L'app Azure Function consente l'invocazione anonima del trigger HTTP

Una HTTP-triggered funzione il cui livello di autorizzazione è impostato su `anonymous` può essere richiamata su Internet senza alcuna chiave di accesso o autenticazione. I trigger HTTP anonimi espongono la logica della funzione a chiamanti non autenticati, il che può causare abusi, esposizione di dati o negazione del portafoglio tramite invocazioni incontrollate. Seguendo i principi di sicurezza standard, richiedi l'autenticazione o le chiavi di accesso per le funzioni, a meno che l'accesso anonimo non sia esplicitamente richiesto. HTTP-triggered

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Richiedi l'autorizzazione per i trigger HTTP

Aumenta il livello di autorizzazione dei trigger HTTP `anonymous` da `function` o `admin` in modo che le richieste debbano includere una chiave di accesso valida e richiedere HTTPS. Per una protezione più efficace, abilita il servizio app Authentication/Authorization o proteggi l'app con Azure API Management. Per ulteriori informazioni, vedi Securing Azure Functions nella documentazione di Microsoft Azure.

Richiedi l'autenticazione con un provider di identità gestito

Poiché le chiavi di accesso sono un controllo di autorizzazione anziché un'autenticazione, abilita App Service Authentication (Easy Auth) con Microsoft Entra ID in modo che i chiamanti debbano presentare un'identità valida. Disabilita anche gli endpoint amministrativi (i `/admin` percorsi) quando non sono necessari. Per ulteriori informazioni, vedi Securing Azure Functions nella documentazione di Microsoft Azure.

Caratteristiche di vulnerabilità per le app Azure Function

Ecco le caratteristiche di vulnerabilità per le app Azure Function e i passaggi di correzione suggeriti.

L'app Azure Function presenta vulnerabilità software sfruttabili in rete con un'alta probabilità di sfruttamento

Le vulnerabilità e le esposizioni comuni (CVE) possono influire sui pacchetti software e sulle dipendenze nell'app Function. Una vulnerabilità ad alta priorità è sfruttabile in rete con un'elevata probabilità di sfruttamento, il che rappresenta una minaccia immediata alla sicurezza perché il codice di exploit potrebbe essere già disponibile al pubblico e utilizzato attivamente dagli aggressori. Correggi tempestivamente queste vulnerabilità per proteggere la tua app Function.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Aggiorna le dipendenze interessate

Esamina i CVE interessati nella scoperta, quindi aggiorna i pacchetti e le dipendenze vulnerabili alle versioni sicure più recenti e ridistribuisci l'app. Mantieni l'app Function su un runtime supportato in modo che gli aggiornamenti di sicurezza della piattaforma continuino ad essere applicati. Per ulteriori informazioni, vedi Microsoft Defender for App Service nella documentazione di Microsoft Azure.

Considerazioni future

Per prevenire eventi futuri, integra la scansione delle dipendenze e delle vulnerabilità nella pipeline di sviluppo e distribuzione e utilizza Microsoft Defender for Cloud per monitorare la tua app per rilevare configurazioni e vulnerabilità. Per ulteriori informazioni, consulta Microsoft Defender for App Service nella documentazione di Microsoft Azure.

L'app Azure Function presenta vulnerabilità software

Le vulnerabilità e le esposizioni comuni (CVE) possono influire sui pacchetti software e sulle dipendenze nell'app Function. Le vulnerabilità non critiche rappresentano punti deboli di sicurezza con gravità o sfruttabilità inferiori rispetto alle vulnerabilità ad alta priorità. Sebbene rappresentino un rischio meno immediato, gli aggressori possono comunque sfruttare le vulnerabilità prive di patch per compromettere la riservatezza, l'integrità o la disponibilità dei dati o per accedere ad altri sistemi. Seguendo le best practice di sicurezza, correggi queste vulnerabilità per proteggere la tua app Function.

Correzione: aggiorna le dipendenze interessate

Aggiorna i pacchetti e le dipendenze vulnerabili alle versioni sicure più recenti e ridistribuisci l'app. Se un aggiornamento non è disponibile, valuta la possibilità di rimuovere o disabilitare il componente vulnerabile fino al rilascio di una patch. Per ulteriori informazioni, vedi Microsoft Defender for App Service nella documentazione di Microsoft Azure.

L'app Azure Function contiene pacchetti software dannosi

I pacchetti dannosi sono componenti software che contengono codice dannoso progettato per compromettere la riservatezza, l'integrità e la disponibilità dei sistemi e dei dati. I pacchetti dannosi rappresentano una minaccia attiva e critica per l'app Function, poiché gli aggressori possono eseguire il codice dannoso automaticamente senza sfruttare una vulnerabilità separata. Seguendo le best practice di sicurezza, rimuovi i pacchetti dannosi per proteggere l'app Function da potenziali attacchi.

Soluzione: analizza e rimuovi i pacchetti dannosi

Esamina i dettagli dei risultati per identificare i pacchetti interessati, rimuoverli dalle dipendenze del progetto, ricostruire da una fonte attendibile e ridistribuire l'app. Dopo la correzione, verifica la catena di fornitura delle dipendenze per confermare che non rimangano componenti dannosi correlati. Per ulteriori informazioni, vedi Microsoft Defender for App Service nella documentazione di Microsoft Azure.

Correzione delle esposizioni per le app Azure Container

AWS Security Hub può generare risultati sull'esposizione per le app Azure Container.

Nella console Security Hub, l'app Azure Container coinvolta nella rilevazione dell'esposizione e le relative informazioni identificative sono elencate nella sezione Risorse dei dettagli dei risultati. A livello di programmazione, è possibile recuperare i dettagli delle risorse con il GetFindingsV2 funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la correzione fornite in questo argomento potrebbero richiedere una consultazione aggiuntiva in altre risorse di Microsoft Azure.

Indice

- Caratteristiche di configurazione errata per le app Azure Container
  - L'app Azure Container dispone di credenziali in chiaro nelle variabili di ambiente
  - L'app Azure Container dispone di un gruppo di sicurezza di rete aperto
  - L'app Azure Container ha un'identità gestita che non prevede il privilegio minimo
  - Al ruolo associato all'app Azure Container è assegnato un ruolo di accesso amministrativo
- Caratteristiche di raggiungibilità per le app Azure Container
  - L'app Azure Container è raggiungibile tramite Internet

Caratteristiche di configurazione errata per le app Azure Container

Ecco le caratteristiche di configurazione errata per le app Azure Container e i passaggi di correzione suggeriti.

L'app Azure Container dispone di credenziali in chiaro nelle variabili di ambiente

L'app Container passa dati segreti, come stringhe di connessione, chiavi API o password, al contenitore come variabili di ambiente in testo normale. La configurazione, i log o un contenitore compromesso possono esporre le credenziali in chiaro nelle variabili di ambiente, il che consente a un utente malintenzionato di riutilizzarle per accedere ad altri sistemi. Seguendo i principi di sicurezza standard, memorizzate i valori sensibili come segreti e fate riferimento ad essi anziché incorporarli in testo normale.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Sposta le credenziali nei segreti

Sostituisci i valori delle variabili di ambiente in testo normale con i segreti delle app Container o i segreti di riferimento archiviati in Azure Key Vault. Aggiorna il contenitore per leggere i valori di tali riferimenti segreti. Ruota tutte le credenziali precedentemente esposte in testo normale. Per ulteriori informazioni, vedi Manage secret in Azure Container Apps nella documentazione di Microsoft Azure.

Usa un'identità gestita laddove possibile

Per le connessioni ai servizi di Azure che la supportano, usa l'identità gestita dell'app Container anziché archiviare affatto un segreto. Per ulteriori informazioni, vedi Identità gestite in Azure Container Apps nella documentazione di Microsoft Azure.

L'app Azure Container dispone di un gruppo di sicurezza di rete aperto

Il gruppo di sicurezza di rete che protegge l'ambiente dell'app Container contiene regole che consentono l'accesso illimitato da qualsiasi fonte (ad esempio, una fonte di `Any` o`0.0.0.0/0`). Un gruppo di sicurezza di rete aperto espone l'ambiente dell'app Container ad accessi non autorizzati da Internet. Seguendo i principi di sicurezza standard, limita le regole del gruppo di sicurezza di rete solo agli indirizzi IP, alle porte e ai protocolli specifici richiesti dal carico di lavoro.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Limita le regole del gruppo di sicurezza di rete

Esamina il gruppo di sicurezza di rete associato alla sottorete dell'ambiente dell'app Container e modifica o rimuovi le regole che consentono l'accesso senza restrizioni. Sostituisci una fonte

generica, ad esempio `Any` con gli intervalli attendibili specifici richiesti dal tuo carico di lavoro. Per ulteriori informazioni, vedi Networking in Azure Container Apps nella documentazione di Microsoft Azure.

Imposta le restrizioni di ingresso IP

Oltre alle regole del gruppo di sicurezza di rete sulla sottorete dell'ambiente, configura le restrizioni di ingresso IP sull'app contenitore stessa per consentire o negare il traffico in entrata in base all'intervallo di indirizzi IP. Per ulteriori informazioni, vedi Configurare le restrizioni di ingresso IP in Azure Container Apps nella documentazione di Microsoft Azure.

L'app Azure Container ha un'identità gestita che non prevede il privilegio minimo

L'app Container ha un'identità gestita a cui viene concesso un accesso maggiore di quello richiesto dal carico di lavoro. Un'identità gestita con privilegi eccessivi aumenta il raggio d'azione se l'app Container è compromessa, perché un utente malintenzionato può agire con tutte le autorizzazioni dell'identità. Seguendo i principi di sicurezza standard, concedi all'identità solo le autorizzazioni necessarie al carico di lavoro, nell'ambito più ristretto.

Correzione: assegna all'identità gestita il privilegio minimo

Esamina le assegnazioni di ruolo concesse all'identità gestita dell'app Container e rimuovi quelle non richieste. Assegna il ruolo predefinito con il minor privilegio nell'ambito più ristretto (risorsa o gruppo di risorse) che soddisfa le tue esigenze. Per ulteriori informazioni, vedi Best practice per Azure RBAC nella documentazione di Microsoft Azure.

Al ruolo associato all'app Azure Container è assegnato un ruolo di accesso amministrativo

L'identità gestita associata all'app Container ha un'assegnazione di ruolo amministrativo (ad esempio `Owner` o`Contributor`) con un ampio ambito. Questa assegnazione in genere concede autorizzazioni ben oltre quelle richieste dal carico di lavoro. Se l'app Container è compromessa, un utente malintenzionato può utilizzare queste autorizzazioni eccessive per spostarsi lateralmente nell'ambiente, accedere ai dati o manipolare le risorse. Seguendo i principi di sicurezza standard, concedi il privilegio minimo assegnando solo le autorizzazioni necessarie all'app.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi e identifica le assegnazioni dei ruoli amministrativi

Nel portale di Azure, esamina le assegnazioni di ruolo per l'identità associata all'app Container. Cerca i ruoli di amministratore privilegiato come`Owner`,, o `ContributorUser Access Administrator`, e i ruoli personalizzati che utilizzano un carattere jolly (`*`) nel loro. `Actions` Per ulteriori informazioni, consulta Elencare le assegnazioni di ruolo di Azure nella documentazione di Microsoft Azure.

Implementazione dell'accesso con privilegi minimi

Sostituisci le assegnazioni dei ruoli amministrativi con il ruolo predefinito con il minor privilegio che concede solo le autorizzazioni richieste dall'app e assegnalo nell'ambito più ristretto che soddisfa le tue esigenze. Per ulteriori informazioni, vedi Best practice per Azure RBAC nella documentazione di Microsoft Azure.

Caratteristiche di raggiungibilità per le app Azure Container

Ecco le caratteristiche di raggiungibilità per le app Azure Container e i passaggi di correzione suggeriti.

L'app Azure Container è raggiungibile tramite Internet

L'app Container è raggiungibile dalla rete Internet pubblica, perché l'ingresso esterno è abilitato (`ingress.external`è impostato su`true`) o perché il suo ambiente ha un indirizzo IP pubblico. La raggiungibilità pubblica aumenta la superficie di attacco dell'app Container e la espone a richieste non autorizzate. Seguendo i principi di sicurezza standard, disabilita l'accesso esterno dove non è richiesto, utilizza un ambiente interno o posiziona l'app dietro un punto di ingresso controllato e autenticato.

Correzione

Intraprendi una o più delle seguenti azioni per ovviare a questa esposizione:

Limita o rimuovi l'ingresso esterno

Imposta l'ingresso su interno se l'app deve essere raggiunta solo dall'interno della tua rete o ambiente virtuale. Se è richiesto l'accesso pubblico, limitalo con restrizioni relative all'indirizzo IP di ingresso. Proteggi l'app con un gateway come Azure Application Gateway o Azure Front Door.

Questi gateway forniscono l'autenticazione e un firewall per le applicazioni Web. Per ulteriori informazioni, vedi Ingress in Azure Container Apps nella documentazione di Microsoft Azure.

Usa un ambiente interno

Per evitare di assegnare un indirizzo IP pubblico, distribuisci l'app Container in un ambiente interno (integrato nella rete virtuale) che utilizza un indirizzo IP privato ed esponi solo gli endpoint che devono essere pubblici attraverso un punto di ingresso controllato. Per ulteriori informazioni, vedi Networking in Azure Container Apps nella documentazione di Microsoft Azure.

Richiedi HTTPS e autenticazione per l'accesso pubblico

Quando l'ingresso deve rimanere pubblico, disabilita le connessioni non sicure (impostate su `allowInsecurefalse`) in modo che il traffico venga servito solo tramite HTTPS. Abilita la funzionalità di autenticazione integrata con Microsoft Entra ID in modo che le richieste non autenticate vengano rifiutate. Per ulteriori informazioni, vedi Autenticazione e autorizzazione in Azure Container Apps nella documentazione di Microsoft Azure.

Correzione delle esposizioni per i cluster di servizi Azure Kubernetes

AWS Security Hub può generare risultati di esposizione per i cluster di Azure Kubernetes Service (AKS).

Nella console di Security Hub, il cluster AKS coinvolto nella rilevazione dell'esposizione e le relative informazioni identificative sono elencati nella sezione Risorse dei dettagli dei risultati. A livello di programmazione, è possibile recuperare i dettagli delle risorse con il GetFindingsV2 funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la correzione fornite in questo argomento potrebbero richiedere una consultazione aggiuntiva in altre risorse di Microsoft Azure.

Indice

- Caratteristiche di configurazione errata per i cluster di servizi Azure Kubernetes
  - Il cluster di servizi Azure Kubernetes esegue una versione di Kubernetes non supportata
  - Il cluster di servizi Azure Kubernetes contiene segreti Kubernetes non crittografati
- Caratteristiche di raggiungibilità per i cluster di servizi Azure Kubernetes
  - Il cluster di servizi Azure Kubernetes consente l'accesso pubblico

Caratteristiche di configurazione errata per i cluster di servizi Azure Kubernetes

Ecco le caratteristiche di configurazione errata per i cluster di servizi Azure Kubernetes e i passaggi di correzione suggeriti.

Il cluster di servizi Azure Kubernetes esegue una versione di Kubernetes non supportata

Il cluster AKS esegue una versione di Kubernetes che non è più supportata da Microsoft. Le versioni di Kubernetes non supportate non ricevono più patch di sicurezza e correzioni di bug, il che lascia irrisolte le vulnerabilità note nel piano di controllo e nei componenti dei nodi ed espone il cluster agli attacchi. Seguendo le best practice di sicurezza, mantieni il cluster su una versione Kubernetes supportata.

Correzione: aggiornamento a una versione Kubernetes supportata

Aggiorna il piano di controllo del cluster e i pool di nodi a una versione Kubernetes supportata. Poiché le versioni secondarie non possono essere ignorate, esegui l'aggiornamento in sequenza tramite ciascuna versione secondaria e applica la patch più recente. Rivedi le modifiche principali per ciascuna versione prima di eseguire l'aggiornamento.

Valuta la possibilità di abilitare gli aggiornamenti automatici per rimanere aggiornati. Per ulteriori informazioni, consulta Versioni di Kubernetes supportate in AKS nella documentazione di Microsoft Azure.

Il cluster di servizi Azure Kubernetes contiene segreti Kubernetes non crittografati

Per impostazione predefinita, il cluster archivia i segreti di Kubernetes nell'archivio dati etcd senza crittografia mediante una chiave controllata dal cliente. Senza la crittografia a riposo tramite un servizio di gestione delle chiavi, chiunque acceda ai dati etcd sottostanti può leggere valori segreti sensibili come credenziali e token. Seguendo le best practice per la protezione dei dati, abilita la crittografia KMS etcd in modo che i segreti di Kubernetes siano crittografati anche quando sono inattivi con una chiave in Azure Key Vault.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Abilita la crittografia KMS etcd

Configura il cluster per utilizzare la crittografia Key Management Service (KMS) etcd con una chiave archiviata in Azure Key Vault. Concedi al cluster le autorizzazioni di crittografia e decrittografia dell'identità sulla chiave. Re-encrypt segreti esistenti dopo aver abilitato la funzionalità. Attiva la protezione da eliminazione graduale ed eliminazione sull'archivio delle chiavi in modo che la chiave non vada persa. Per ulteriori informazioni, vedi la crittografia KMS etcd in AKS nella documentazione di Microsoft Azure.

Attiva la protezione da eliminazione graduale ed eliminazione sul key vault in modo che la chiave non possa essere persa. Per ulteriori informazioni, consulta la crittografia KMS etcd in AKS nella documentazione di Microsoft Azure.

Archivia i segreti in Azure Key Vault

Per evitare del tutto di archiviare valori sensibili come segreti Kubernetes in etcd, usa il provider Azure Key Vault per il driver CSI Secrets Store per montare segreti, chiavi e certificati da Azure Key Vault nei pod in fase di esecuzione. Per ulteriori informazioni, vedi Azure Key Vault provider for Secrets Store CSI Driver nella documentazione di Microsoft Azure.

Caratteristiche di raggiungibilità per i cluster di servizi Azure Kubernetes

Ecco le caratteristiche di raggiungibilità per i cluster di servizi Azure Kubernetes e i passaggi di riparazione suggeriti.

Il cluster di servizi Azure Kubernetes consente l'accesso pubblico

Il server API è l'endpoint che usi per comunicare con il piano di controllo Kubernetes del tuo cluster. Il cluster è raggiungibile da Internet quando l'endpoint del server API è pubblico o quando i carichi di lavoro sono esposti tramite un load balancer o un ingresso pubblico. Gli endpoint pubblici aumentano la superficie di attacco e il rischio di accesso non autorizzato al server API Kubernetes. Gli aggressori possono potenzialmente accedere o modificare le risorse del cluster e leggere dati sensibili. Seguendo le best practice di sicurezza, limita l'accesso al server API e ai carichi di lavoro del cluster ai soli intervalli IP necessari.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Limita l'accesso al server API

Utilizza un cluster privato in modo che il server API sia raggiungibile solo dall'interno della tua rete virtuale o configura gli intervalli IP autorizzati per limitare gli indirizzi di origine che possono raggiungere l'endpoint pubblico del server API. Per ulteriori informazioni, consulta Private Azure Kubernetes Service Clusters nella documentazione di Microsoft Azure.

Limita l'esposizione pubblica dei carichi di lavoro

Esamina i servizi esposti tramite sistemi di bilanciamento del carico o ingress pubblici e limita o rimuovi l'esposizione del pubblico laddove non sia richiesta. Utilizza sistemi di bilanciamento del carico interni, regole dei gruppi di sicurezza di rete e un firewall per applicazioni Web su un punto di ingresso controllato per i carichi di lavoro che devono essere raggiunti da Internet. Per ulteriori informazioni, consulta Networking concepts for AKS nella documentazione di Microsoft Azure.

Correzione delle esposizioni per gli utenti di Azure Graph

AWS Security Hub può generare risultati sull'esposizione per gli utenti di Azure Graph.

Nella console di Security Hub, l'utente di Azure Graph coinvolto nella rilevazione dell'esposizione e le relative informazioni identificative sono elencati nella sezione Risorse dei dettagli dei risultati. A livello di programmazione, è possibile recuperare i dettagli delle risorse con il GetFindingsV2 funzionamento dell'API CSPM di Security Hub.

Dopo aver identificato la risorsa coinvolta nella rilevazione dell'esposizione, puoi eliminarla se non ti serve. L'eliminazione di una risorsa non essenziale può ridurre il profilo di esposizione e AWS i costi. Se la risorsa è essenziale, segui questi passaggi correttivi consigliati per ridurre il rischio. Gli argomenti relativi alla correzione sono suddivisi in base al tipo di caratteristica.

Un singolo risultato di esposizione contiene i problemi identificati in più argomenti di correzione. Al contrario, è possibile risolvere un rilevamento dell'esposizione e ridurne il livello di gravità affrontando un solo argomento relativo alla correzione. L'approccio alla correzione del rischio dipende dai requisiti organizzativi e dai carichi di lavoro.

> **Note**
>
> Le linee guida per la correzione fornite in questo argomento potrebbero richiedere una consultazione aggiuntiva in altre risorse di Microsoft Azure.

Indice

- Caratteristiche di configurazione errata per gli utenti di Azure Graph
  - Al ruolo associato all'utente di Azure Graph è assegnato un ruolo di accesso amministrativo
  - L'utente di Azure Graph non ha l'MFA abilitato

Caratteristiche di configurazione errata per gli utenti di Azure Graph

Ecco le caratteristiche di configurazione errata per gli utenti di Azure Graph e i passaggi di correzione suggeriti.

Al ruolo associato all'utente di Azure Graph è assegnato un ruolo di accesso amministrativo

L'utente di Azure Graph ha un'assegnazione di ruolo amministrativa di Azure Role Based Access Control (Azure RBAC), ad esempio, o. `Owner` `Contributor` `User Access Administrator` L'assegnazione ha spesso un ambito ampio, ad esempio una sottoscrizione o un gruppo di gestione. Le assegnazioni dei ruoli amministrativi concedono ampie autorizzazioni, pertanto un utente malintenzionato può utilizzare un account utente compromesso per spostarsi lateralmente, accedere ai dati o manipolare le risorse nell'ambiente. Seguendo i principi di sicurezza standard, concedi il privilegio minimo e limita le assegnazioni dei ruoli di amministratore con privilegi.

Correzione

Intraprendi una o più delle seguenti azioni per risolvere questa esposizione:

Rivedi e identifica le assegnazioni dei ruoli amministrativi

Nel portale di Azure, esamina le assegnazioni di ruolo dell'utente. Cerca i ruoli di amministratore con privilegi`Owner`, ad esempio`Contributor`, o`User Access Administrator`, e i ruoli personalizzati che utilizzano un carattere jolly (`*`) nel loro. `Actions` Per ulteriori informazioni, consulta Elencare le assegnazioni di ruolo di Azure nella documentazione di Microsoft Azure.

Implementazione dell'accesso con privilegi minimi

Rimuovi le assegnazioni di ruolo privilegiate non necessarie e sostituiscile con il ruolo predefinito con privilegi meno privilegiati, assegnato nell'ambito più ristretto. Preferisci i ruoli professionali rispetto ai ruoli di amministratore con privilegi. Riduci al minimo il numero di titolari dell'abbonamento: Microsoft ne consiglia non più di tre.

Assegna i ruoli ai gruppi anziché ai singoli utenti. Usa Microsoft Entra Privileged Identity Management per rendere i ruoli privilegiati idonei all'attivazione just-in-time e limitata nel tempo invece di

concedere l'accesso permanente. Per ulteriori informazioni, vedi Best practice per Azure RBAC nella documentazione di Microsoft Azure.

L'utente di Azure Graph non ha l'MFA abilitato

L'utente di Azure Graph può accedere in modo interattivo senza autenticazione a più fattori (MFA). Senza MFA, un account è protetto solo da una password, il che lo rende vulnerabile agli attacchi di phishing, password spray e furto di credenziali. Una sola password compromessa è sufficiente per consentire a un utente malintenzionato di accedere. Seguendo i principi di sicurezza standard, richiedi l'autenticazione MFA per tutti gli utenti con accesso interattivo.

Soluzione: richiedi l'autenticazione a più fattori

Richiedi l'autenticazione a più fattori per l'utente tramite una policy di accesso condizionale di Microsoft Entra. Per un'ampia copertura, abilita le impostazioni di sicurezza predefinite o una politica di accesso condizionale che richieda l'autenticazione a più fattori per tutti gli utenti. Dai la priorità a una policy dedicata per gli amministratori.

Ove possibile, richiedi metodi resistenti al phishing, come chiavi di sicurezza FIDO2, passkey o Windows Hello for Business, tramite un sistema di autenticazione con accesso condizionale. Evita di autorizzare metodi suscettibili di phishing come SMS o voce. Per ulteriori informazioni, vedi Pianificare una distribuzione dell'autenticazione a più fattori nella documentazione di Microsoft Azure.

Comprendere i risultati degli accessi non utilizzati in Security Hub

Security Hub utilizza IAM Access Analyzer per identificare le autorizzazioni, i ruoli, le chiavi di accesso e le password IAM non utilizzati nel tuo account. Questi risultati ti aiutano a implementare la best practice di sicurezza dell'accesso con privilegi minimi evidenziando i principi e le autorizzazioni IAM che non vengono utilizzati attivamente. Questa funzionalità viene fornita a tutti i clienti di Security Hub senza costi aggiuntivi.

Come funziona l'analisi degli accessi non utilizzati

Quando abiliti Security Hub, il servizio crea automaticamente un IAM Access Analyzer collegato al servizio nel tuo account. Questo analizzatore valuta tutti i principali IAM (ruoli e utenti) rispetto ai dati delle AWS CloudTrail attività per determinare quali principi e autorizzazioni non sono stati utilizzati entro un periodo di riferimento di 90 giorni. Il periodo di lookback non è configurabile.

IAM Access Analyzer rivaluta tutti i risultati attivi ogni 24 ore. Quando un principale o un'autorizzazione precedentemente inutilizzati diventano attivi, il risultato corrispondente viene risolto automaticamente.

L'analizzatore di accesso inutilizzato viene eseguito negli Stati Uniti orientali (Virginia settentrionale) perché IAM è un servizio globale. Security Hub replica i risultati in tutte le regioni in cui hai abilitato Security Hub. Non è necessario abilitare Security Hub negli Stati Uniti orientali (Virginia settentrionale) per far funzionare l'analizzatore.

Tipi di ricerca di accesso non utilizzati

Security Hub genera quattro tipi di rilevazioni di accesso non utilizzate:

Tipo di risultato	Description	Risorsa valutata
Ruolo IAM non utilizzato	Un ruolo IAM che non è stato assunto entro il periodo di lookback di 90 giorni.	Ruolo IAM
UnusedIAM UserAccessKey	Una chiave di accesso utente IAM che non è stata utilizzata per firmare le richieste API entro il periodo di lookback di 90 giorni.	Utente IAM
UnusedIAM UserPassword	Una password utente IAM che non è stata utilizzata per l'accesso alla console entro il periodo di lookback di 90 giorni.	Utente IAM
UnusedPermission	Azioni IAM specifiche concesse a un ruolo o a un utente ma che non sono state richiamate entro il periodo di lookback di 90 giorni.	Ruolo IAM o utente IAM

Service-linked analizzatore

L'IAM Access Analyzer creato da Security Hub è un analizzatore collegato ai servizi. Puoi visualizzarlo nella console di IAM Access Analyzer, ma non puoi modificarlo o eliminarlo mentre Security Hub è abilitato.

Quando disabiliti Security Hub in tutte le regioni, l'analizzatore collegato al servizio viene eliminato automaticamente. Se l'eliminazione automatica non riesce, puoi eliminare l'analizzatore richiamando

l'operazione API IAM Access Analyzer. `DeleteServiceLinkedAnalyzer` Questa operazione ha esito positivo solo dopo che Security Hub è stato completamente disabilitato per il tuo account.

L'analizzatore collegato al servizio è separato da qualsiasi analizzatore gestito dal cliente che potresti aver creato indipendentemente in IAM Access Analyzer. La creazione o l'eliminazione di analizzatori gestiti dal cliente non influisce sull'analizzatore collegato al servizio e viceversa.

Visualizzazione dei risultati di accesso non utilizzati

I risultati degli accessi non utilizzati vengono visualizzati nella console di Security Hub insieme ad altri risultati di Security Hub. Puoi filtrare i risultati per tipo per visualizzare solo i risultati di accesso non utilizzati. I risultati di accesso non utilizzati sono formattati nell'Open Cybersecurity Schema Framework (OCSF), lo stesso formato utilizzato da tutti i risultati di Security Hub.

Per UnusedPermission quanto riguarda i risultati, se rimuovi alcune autorizzazioni inutilizzate dalla policy eccessivamente permissiva, ma non tutte, Security Hub chiude la ricerca esistente e ne crea una nuova per la policy rivista se è ancora eccessivamente permissiva.

I risultati degli accessi non utilizzati sono accessibili anche dalla console IAM Access Analyzer. I risultati di accesso non utilizzati nella console IAM Access Analyzer sono di sola lettura e sono visibili solo nella regione Stati Uniti orientali (Virginia settentrionale).

Accesso non utilizzato ai risultati dell'esposizione

Le informazioni di accesso non utilizzate possono apparire come tratti contestuali nei risultati dell'esposizione di Security Hub. Quando un ruolo IAM collegato a una risorsa dispone di autorizzazioni inutilizzate, il risultato dell'esposizione include queste autorizzazioni come contesto supplementare. Questo ti aiuta a comprendere il potenziale raggio di diffusione di una vulnerabilità: una risorsa con un ruolo IAM eccessivamente privilegiato presenta un rischio maggiore rispetto a una con autorizzazioni con privilegi minimi.

I seguenti tipi di risorse possono mostrare tratti contestuali di accesso non utilizzati nei risultati dell'esposizione:

- Istanze Amazon Elastic Compute Cloud
- AWS Lambda funzioni
- servizi Amazon Elastic Container Service
- Cluster Amazon Elastic Kubernetes Service
- Utenti IAM (direttamente)

Per ulteriori informazioni sui risultati dell'esposizione, vedereEsiti relativi alle esposizioni in Security Hub.

Raccomandazioni politiche per le autorizzazioni non utilizzate

Per UnusedPermission i risultati, Security Hub può generare raccomandazioni sulle politiche con privilegi minimi. Questi consigli mostrano una politica di sostituzione ridotta che mantiene solo le autorizzazioni effettivamente utilizzate dal principale. Per ulteriori informazioni, consulta Generazione di raccomandazioni politiche per i risultati di accesso non utilizzati.

Prezzi

L'IAM Access Analyzer collegato al servizio viene fornito a tutti i clienti di Security Hub senza costi aggiuntivi. Non ti vengono addebitati separatamente l'analizzatore o i risultati di accesso non utilizzati.

Generazione di raccomandazioni politiche per i risultati di accesso non utilizzati

Per individuare le autorizzazioni non utilizzate, Security Hub può generare raccomandazioni sulle politiche con privilegi minimi che mostrano una politica sostitutiva limitata. La raccomandazione valuta ogni policy associata all'entità IAM e ne genera una sostitutiva che mantiene solo le autorizzazioni effettivamente utilizzate dal principale. Questa funzionalità viene fornita a tutti i clienti di Security Hub senza costi aggiuntivi.

Come funzionano i consigli sulle policy

La generazione delle raccomandazioni politiche è un'operazione asincrona. Per generare e recuperare un consiglio:

1. Recupera le autorizzazioni non utilizzate rilevate da Security Hub utilizzando l'operazione API. `GetFindingsV2` Annota il `metadata.uid` campo riportato nella scoperta.
2. Chiama `GenerateRecommendedPolicyV2` con i risultati`metadata.uid`. Questo avvia la generazione della raccomandazione, che in genere viene completata entro 20 secondi.
3. Effettua il `GetRecommendedPolicyV2` polling con la stessa `metadata.uid` finché non ritorna il campo`status`. `SUCCEEDED`
4. La risposta contiene uno o più passaggi consigliati. Ogni passaggio specifica uno `recommendedAction` dei due `CREATE_POLICY` (creare e allegare una politica di sostituzione

con un ambito limitato) o `DETACH_POLICY` (rimuovere la politica originale con privilegi eccessivi). Per quanto riguarda `CREATE_POLICY` i passaggi, la risposta include sia il JSON che il `existingPolicy` JSON in modo da poterli confrontare`recommendedPolicy`.

È necessario chiamare `GenerateRecommendedPolicyV2` prima di chiamare `GetRecommendedPolicyV2` se in precedenza non è stato generato un consiglio per tale risultato.

Chi può generare consigli

Sia il proprietario dell'account che gli amministratori delegati possono chiamare queste operazioni API:

- I proprietari degli account possono generare e visualizzare nel proprio account consigli per i risultati delle autorizzazioni non utilizzate.
- Gli amministratori delegati possono generare e visualizzare consigli per i risultati delle autorizzazioni non utilizzate di qualsiasi account membro all'interno della propria organizzazione.

Se non sei un amministratore delegato e il risultato appartiene a un altro account, l'operazione API restituisce un errore. `AccessDeniedException`

Ciclo di vita dei consigli

- I consigli vengono memorizzati nella cache per 90 giorni e rimangono disponibili finché il risultato è attivo (non chiuso). Tuttavia, una chiamata `GenerateRecommendedPolicyV2` ripetuta invalida la cache e avvia un nuovo processo che sostituisce la policy memorizzata nella cache. Chiama `GenerateRecommendedPolicyV2` solo una volta per ricerca.
- La raccomandazione segue uno schema «stacca e attacca». Non modifica le politiche IAM esistenti. Rivedi la policy consigliata e la applichi manualmente nella console IAM o tramite l'API IAM.
- Se il risultato viene risolto (ad esempio, perché ora vengono utilizzate le autorizzazioni precedentemente non utilizzate), il consiglio non è più disponibile.

Casi di errore

Le operazioni API restituiscono errori nelle seguenti situazioni:

- Il problema è stato risolto `InvalidInputException` (HTTP 400).

- Il risultato non è un risultato di autorizzazioni inutilizzato `InvalidInputException` (HTTP 400).
- L'entità IAM è stata creata tramite il set di autorizzazioni IAM Identity Center. Le politiche per i principali dei set di autorizzazioni non possono essere modificate direttamente. La raccomandazione restituisce uno `FAILED` stato con una spiegazione.
- Il chiamante non è un amministratore delegato e il risultato appartiene a un altro account `AccessDeniedException` (HTTP 403).
- Non è stata ancora generata alcuna raccomandazione e si chiama `GetRecommendedPolicyV2` senza prima chiamare `ResourceNotFoundException` (HTTP `GenerateRecommendedPolicyV2` 404).

Utilizzo della console

Nella console Security Hub, puoi generare una raccomandazione relativa alle policy visualizzando la ricerca delle autorizzazioni non utilizzate e scegliendo la scheda Riparazione. La console mostra uno spinner di caricamento durante la creazione del consiglio. Quando il consiglio è pronto, puoi scegliere Anteprima per visualizzare un confronto fianco a fianco tra la tua politica attuale e la sostituzione consigliata con il privilegio minimo. Puoi copiare la policy consigliata in formato JSON.

Guida di riferimento alle API

- GenerateRecommendedPolicyV2— Avvia la generazione asincrona di una policy con privilegi minimi per la ricerca delle autorizzazioni non utilizzate. Accetta `metadata.uid` i risultati come input. In caso di successo, restituisce HTTP 200 con un corpo vuoto.
- GetRecommendedPolicyV2— Recupera la raccomandazione politica generata. Accetta i risultati `metadata.uid` come input. Supporta l'impaginazione con `maxResults` (1—100) e parametri. `nextToken` Restituisce lo stato del consiglio (`IN_PROGRESS`,`SUCCEEDED`, o`FAILED`), i passaggi del consiglio, l'ARN della risorsa ed eventuali errori.

Per una documentazione dettagliata sull'API, consulta il Security Hub API Reference.

Scansione della rete in Security Hub

La scansione della rete è una funzionalità opzionale di Security Hub che esegue test attivi di raggiungibilità della rete sulle risorse cloud. Control-plane l'analisi valuta i gruppi di sicurezza, gli elenchi di controllo dell'accesso alla rete (NACL) e le tabelle di routing per determinare cosa

potrebbe essere raggiungibile. La scansione della rete va oltre rilevando ciò che è effettivamente raggiungibile. Esamina le tue risorse esterne ai tuoi account per identificare le porte aperte e i servizi in esecuzione.

Tutte le scansioni provengono da indirizzi AWS IP di proprietà e rispondono a due domande: questa risorsa è raggiungibile da Internet? Se raggiungibile, cosa è in esecuzione? Network Scanning pubblica i risultati come risultati OCSF autonomi in Security Hub con prove di scansione.

Tipi di risorse supportati

Network Scanning supporta i seguenti tipi di risorse.

Fornitore di servizi cloud	Tipo di risorsa
AWS	Istanza EC2 (con IP pubblico)
AWS	IP elastico (EIP)
AWS	Network Load Balancer (NLB)
AWS	Application Load Balancer (ALB)
AWS	Load Balancer classico (CLB)
Azure	Indirizzo IP pubblico

> **Note**
>
> Network Scanning analizza ogni tipo di risorsa in modo indipendente. Per i sistemi di bilanciamento del carico, Network Scanning risolve e analizza il nome DNS. Network Scanning esegue la scansione delle singole istanze EC2 su un sistema di bilanciamento del carico solo se dispongono di un proprio IP o EIP pubblico.

Abilita la scansione di rete

Per abilitare la scansione in rete, Security Hub deve essere abilitato sul tuo account. È possibile abilitare la scansione della rete tramite una politica di configurazione o per singoli account.

Account aziendali (consigliato): abilita la scansione della rete tra gli account e le regioni dell'organizzazione creando o modificando una politica di configurazione. Per ulteriori informazioni sulla modifica di una politica di configurazione, vedere Modifica di una politica di configurazione. Quando Network Scanning è abilitato tramite un criterio di configurazione, gli account dei membri non possono disattivare la funzionalità.

Account individuali: per gli account che non sono gestiti da una politica di configurazione, è possibile abilitare la scansione della rete utilizzando uno dei seguenti metodi.

> **Note**
>
> Abilitando la scansione della rete, autorizzi Security Hub a eseguire una scansione attiva della rete sulle risorse nei tuoi AWS ambienti e negli ambienti Azure. Ciò include i tentativi di connessione alla porta TCP, l'identificazione di applicazioni e protocolli e la raccolta di banner di servizio, intestazioni HTTP e metadati dei certificati TLS.

Security Hub console

Per abilitare la scansione in rete

1. Aprire la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Nel pannello di navigazione, scegli Impostazioni generali.
3. Individua la sezione Network Scanning.
4. Scegli Abilita .
5. Conferma l'autorizzazione per procedere con la scansione attiva della rete.

Security Hub API

Richiama l'`EnableSecurityHubFeatureV2`API con il nome `NETWORK_SCANNING` della funzionalità.

> **Note**
>
> La chiamata a questa API quando Network Scanning è già abilitata restituisce una risposta 200. Il servizio conserva il `UpdatedAt` timestamp dell'abilitazione originale.

AWS CLI

Esegui il comando seguente per abilitare la scansione in rete:

```
aws securityhub enable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

Come funziona la scansione in rete

Dopo aver abilitato la scansione in rete, si verifica quanto segue:

- Network Scanning esegue la scansione delle risorse esistenti entro circa 24 ore dall'attivazione della funzionalità.
- Network Scanning analizza le nuove risorse poco dopo che Security Hub riceve la notifica della risorsa creata.
- Network Scanning esegue nuovamente la scansione delle risorse quando vengono apportate determinate modifiche al piano di controllo idoneo a una risorsa idonea alla scansione.
- Network Scanning esegue nuovamente la scansione delle risorse attive all'incirca ogni 12 ore per rilevare le modifiche alla raggiungibilità.

Le risorse temporanee o di breve durata potrebbero non essere scansionate prima di essere terminate.

Risultati della scansione di rete

Network Scanning pubblica i risultati in formato Open Cybersecurity Schema Framework (OCSF), utilizzando l'estensione AWS OCSF, e vengono visualizzati insieme ad altri risultati di Security Hub. La scansione della rete determina se una risorsa dispone o meno di porte raggiungibili. Se non esiste un risultato per un tipo di risorsa supportato, Network Scanning non ha ancora analizzato la risorsa.

Risultati relativi alle porte raggiungibili

Ogni risultato rappresenta una singola porta raggiungibile su una specifica combinazione di risorse e indirizzi. La `port_scan_result_list` sezione di un risultato OCSF contiene i risultati della scansione. Gli esempi seguenti mostrano le informazioni restituite per una risorsa raggiungibile:

```
"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
    }
  ],
```

Risultati informativi relativi all'assenza di porte aperte

La scansione di rete crea un risultato quando non rileva alcuna porta aperta su una risorsa. Questo risultato ha una gravità di `Informational` e non richiede alcuna azione. Conferma che Network Scanning ha analizzato la risorsa.

Il risultato informativo rimane aperto in Security Hub finché non si elimina la risorsa o finché Network Scanning non rileva porte aperte sulla risorsa. Quando Network Scanning identifica le porte aperte su una risorsa con un risultato informativo, chiude il risultato informativo. Quindi crea un risultato per ogni porta aperta.

I risultati informativi relativi all'assenza di porte aperte riguardano le porte attualmente supportate da Network Scanning. Per un elenco delle porte supportate, vederethe section called "Porte supportate".

Ricerca degli eventi del ciclo di vita

La tabella seguente descrive il ciclo di vita di un risultato di Network Scanning.

Event	Cosa succede
Nessuna porta aperta rilevata	La scansione in rete crea un `Informational` risultato che non richiede alcuna azione
Porte aperte rilevate sulla risorsa con ricerca informativa	La scansione in rete chiude il risultato informativo e crea un risultato per ogni porta aperta
Porta rilevata per la prima volta come raggiungibile	Network Scanning crea e pubblica una nuova scoperta
Porta ancora raggiungibile su rescan (nessuna modifica)	Network Scanning aggiorna periodicamente il risultato
La porta è ancora raggiungibile ma le prove sono cambiate	Network Scanning ripubblica la scoperta con prove aggiornate
Porta non più raggiungibile	La ricerca rimane aperta fino a quando la successiv a scansione non confermerà che la porta non è raggiungibile

Event	Cosa succede
Risorsa terminata o eliminata	Network Scanning chiude tutti i risultati relativi alla risorsa impostando l'attributo su `activity_name` `Close`
Indirizzo IP rimosso dalla risorsa	La scansione di rete chiude i risultati relativi a quell'IP specifico
Scansione di rete disattivata	La scansione in rete non produce nuovi risultati; i risultati esistenti rimangono invariati fino a esaurimento
Security Hub disattivato	Non hai più accesso ai risultati

Se una porta è raggiungibile in modo intermittente, Network Scanning basa i risultati su prove positive al momento della scansione. Dopo aver risolto un problema (ad esempio, chiudendo una regola del firewall o interrompendo un servizio), Network Scanning chiude il risultato alla scansione successiva.

La disattivazione della scansione in rete non comporta la chiusura immediata dei risultati. I risultati esistenti rimangono visibili fino a esaurimento nel normale ciclo di vita dei risultati di Security Hub.

> **Note**
>
> Quando si collega un indirizzo IP elastico (EIP) a un'istanza Amazon EC2, Network Scanning produce risultati sulla risorsa EIP. L'EIP è la risorsa IP di primo livello proprietaria dell'indirizzo. Per le risorse Network Load Balancer (NLB), il nome DNS e gli EIP associati sono punti di ingresso alla rete distinti, pertanto Network Scanning produce risultati separati per ciascuno.

Scansiona le prove

Quando Network Scanning rileva che una porta è raggiungibile, il risultato include prove sul servizio raggiungibile. È possibile raccogliere i seguenti tipi di prove:

Banner TCP

Byte iniziali inviati dal servizio al momento della connessione, ad esempio una stringa di versione SSH.

Metadati HTTP

Intestazioni di risposta e codice di stato HTTP.

Certificato TLS

Nome comune (CN), emittente, data di scadenza e stato autofirmato.

Rilevamento del servizio

Applicazione o protocollo identificato in esecuzione sulla porta.

Esclusione delle risorse dalla scansione

Per escludere una risorsa dalla scansione in rete, aggiungete la chiave tag `SecurityHubNetworkScanExclusion` alla risorsa. Il valore del tag può essere qualsiasi valore o vuoto.

È necessario applicare il tag alla risorsa effettiva con l'IP pubblico scansionabile:

- Per un EIP collegato a un'istanza EC2, contrassegna l'EIP, non l'istanza EC2.
- Per un'istanza EC2 con solo un IP pubblico (senza EIP), contrassegna l'istanza EC2.
- Per un sistema di bilanciamento del carico, contrassegna il load balancer e tutti i target con singoli IP pubblici.

Quando aggiungi il tag di esclusione, Network Scanning interrompe le scansioni future e chiude i risultati attivi per quella risorsa. La rimozione del tag rende la risorsa idonea per la scansione nuovamente.

Porte supportate

Network Scanning analizza le seguenti porte TCP note su risorse idonee.

```
21, 22, 23, 25, 53, 80, 110, 143, 443, 445, 1433, 3306, 3389, 5432,
5900, 6379, 8080, 8443, 9200, 27017
```

Multi-cloud supporto

La scansione di rete supporta gli indirizzi IP pubblici di Azure. Per analizzare le risorse di Azure, crea un connettore Security Hub per il tuo ambiente Azure. Per ulteriori informazioni sull'integrazione con Microsoft Azure, vedi Integrating Security Hub with Microsoft Azure.

Il comportamento di scansione, le prove e i risultati delle risorse di Azure sono identici alle risorse. AWS I risultati vengono visualizzati insieme ai AWS risultati con i metadati appropriati del provider di cloud e della regione.

Disponibilità nelle regioni

La scansione della rete è disponibile nelle AWS regioni commerciali in cui è disponibile Security Hub.

Disattiva la scansione di rete

Se l'organizzazione utilizza criteri di configurazione, l'amministratore delegato può disabilitare la scansione della rete per account e regioni specifici modificando i criteri di configurazione. Per ulteriori informazioni sulla modifica di una politica di configurazione, vedere Modifica di una politica di configurazione. Quando modifichi la policy, seleziona la funzionalità di scansione della rete, scegli Disabilita, quindi specifica gli account e le regioni in cui desideri disattivare la scansione.

Per gli account che non sono gestiti da un criterio di configurazione, puoi disattivare la scansione in rete utilizzando uno dei seguenti metodi.

Security Hub console

Per disattivare la scansione in rete

1. Aprire la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Nel pannello di navigazione, scegli Impostazioni generali.
3. Individua la sezione Network Scanning.
4. Scegliere Disabilita.
5. Conferma di voler disattivare la scansione in rete.

Security Hub API

Richiama l'`DisableSecurityHubFeatureV2`API con il nome `NETWORK_SCANNING` della funzionalità.

AWS CLI

Esegui il comando seguente per disabilitare la scansione in rete:

```
aws securityhub disable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

Quando si disattiva la scansione in rete:

- La scansione in rete non attiva nuove scansioni.
- I risultati esistenti rimangono visibili fino a esaurimento nel normale ciclo di vita dei risultati di Security Hub.
- La scansione in rete completa tutte le scansioni già in corso.

Piani di riparazione in Security Hub

Un piano di correzione in AWS Security Hub raggruppa i risultati relativi all'esposizione che condividono una causa principale. Ogni piano si rivolge a una singola risorsa nell' AWS ambiente. Quando si corregge tale risorsa, è possibile risolvere o ridurre la gravità di più esposizioni contemporaneamente.

Le esposizioni correlate spesso derivano dallo stesso problema di fondo, ad esempio un'errata configurazione o un'impostazione eccessivamente permissiva su una risorsa. Invece di elencare un'azione separata per ogni esposizione, un piano di riparazione raggruppa queste esposizioni in base alla causa condivisa. Affrontate la fonte una sola volta e riducete la maggior parte dei rischi con il minor numero di azioni.

Per ulteriori informazioni sui risultati dell'esposizione, vedereEsiti relativi alle esposizioni in Security Hub.

In che modo Security Hub crea piani di riparazione

Security Hub crea piani di riparazione in base ai risultati sull'esposizione nel tuo account. Genera un piano per ogni combinazione di risorsa target e caratteristica di esposizione che è in grado di affrontare.

Security Hub dà priorità ai tuoi piani in modo che quelli che riducono il maggior rischio vengano visualizzati per primi. La priorità ti aiuta a decidere su cosa lavorare per primo.

Quando Security Hub rileva una nuova esposizione, un piano per essa potrebbe non apparire immediatamente.

Dettagli del piano di riparazione

Ogni piano di riparazione include i seguenti dettagli.

- Priorità: con quanta urgenza è necessario agire in base al piano. Il valore è Critico, Alto, Medio o Basso.
- Stato: lo stato attuale del piano. Il valore è Nuovo, Aggiornato o Risolto. Per informazioni sul significato di ogni stato, consultaStato del piano di risanamento.
- Impatto: in che modo il piano modifica le tue esposizioni. Un piano può risolvere completamente alcune esposizioni, ridurre la gravità di altre e affrontarne altre senza modificarne la gravità. Il valore indica il conteggio in ogni caso.
- Implementazione: indica se la correzione si applica immediatamente o richiede una distribuzione. Il valore è Immediato o Richiede l'implementazione.
- Azione: la modifica consigliata dal piano.
- Caratteristica: la caratteristica di esposizione affrontata dal piano.
- Risorsa di destinazione: la risorsa corretta dal piano e il relativo tipo di risorsa.
- Account e regione: Account AWS la proprietaria della risorsa di destinazione e della relativa Regione AWS.

Un piano indica anche l'ambito interessato, il livello di rischio, la reversibilità, il livello di automazione e se è necessaria una revisione umana, quando le linee guida lo prevedono.

Stato del piano di risanamento

Security Hub imposta lo stato di ogni piano. Non puoi cambiarlo direttamente.

Novità

Security Hub ha creato il piano e da allora il piano non è cambiato.

Aggiornato

Il piano è cambiato dopo che Security Hub lo ha creato. Ad esempio, la priorità, l'impatto, le esposizioni interessate o le linee guida sono cambiate. Il piano mantiene questo stato fino a quando non viene risolto.

Risolto

Il piano non deve più essere applicato. Security Hub risolve un piano quando non lo genera più in base alle esposizioni correnti. Ciò accade quando le esposizioni del piano vengono risolte, eliminate o archiviate, quando la loro gravità diventa informativa o quando non hanno più la caratteristica a cui si riferisce il piano.

Un piano risolto non significa sempre che i risultati relativi all'esposizione siano stati risolti. Ad esempio, esiste ancora un'esposizione la cui gravità cambia in Informativa.

Un piano risolto rimane nell'elenco per circa 14 giorni, quindi Security Hub lo rimuove. Se il piano deve essere riapplicato, il suo stato diventa Nuovo.

Linee guida per la riparazione

Ogni piano di riparazione include linee guida che descrivono come risolvere il problema. Apri un piano per leggerne le linee guida nella sezione Guida della scheda Panoramica.

> **Note**
>
> Security Hub descrive i passaggi e li applichi tu stesso. Security Hub non modifica le tue risorse per te.

La guida raggruppa i passaggi in fasi, ad esempio Prerequisite, Snapshot, Fix, Verify e Done. Le fasi e il contenuto di ciascuna di esse derivano dalla guida per la risorsa target.

Un passaggio può anche includere un rollback, che descrive come annullarlo.

La guida può includere comandi di esempio in più di un formato, come Azure CLI AWS CLI, Python, Terraform, CDK CloudFormation, Bicep e modello ARM. I formati disponibili provengono dalla guida per la risorsa di destinazione. Se non è disponibile alcuna guida per la risorsa di destinazione, la sezione lo riporta invece.

Visualizzazione dei piani di riparazione

Puoi visualizzare i tuoi piani di riparazione nella pagina Piani di riparazione nella console Security Hub.

Per visualizzare i piani di riparazione

1. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Nel riquadro di navigazione, in Risposta, scegli Riparazioni.

La pagina Piani di riparazione elenca i piani di riparazione in una tabella. Ogni riga mostra l'azione consigliata, la priorità del piano, la risorsa di destinazione con il relativo Regione AWS e l'impatto Account AWS, lo stato e l'implementazione del piano. Per sapere cosa significano, vediDettagli del piano di riparazione.

Non puoi ordinare l'elenco per colonna.

Filtrare i piani di riparazione

Per restringere l'elenco, usa la barra dei piani di riparazione dei filtri. È possibile filtrare in base alle seguenti proprietà:

- Priorità
- Stato
- Tipo di risorsa
- Fornitore di servizi cloud
- ID della risorsa di destinazione
- Account

Questi filtri hanno i seguenti limiti:

- Ogni filtro corrisponde ai valori solo in base all'uguaglianza. Non puoi utilizzare corrispondenze o intervalli parziali.
- Puoi applicare fino a due filtri alla volta. Security Hub li combina con`AND`, quindi un piano deve corrispondere a entrambi i filtri per apparire.
- I valori distinguono tra maiuscole e minuscole Per Tipo di risorsa, inserisci il tipo completo così come appare nell'elenco, ad esempio`AWS::EC2::Instance`.

Visualizzazione delle esposizioni influenzate da un piano

Quando si apre un piano di riparazione, il pannello dei dettagli include una scheda Esposizioni interessate. Questa scheda elenca i risultati dell'esposizione affrontati dal piano. Per ogni esposizione, mostra il titolo dell'esposizione, il modo in cui il piano lo modifica e la conseguente variazione di gravità.

Un'esposizione che il piano affronta senza ridurne la gravità mostra un unico valore di gravità anziché una modifica.

Se un piano influisce su più esposizioni di quelle mostrate nella scheda, la scheda riporta quante esposizioni sono visualizzate.

Visualizzazione dei piani di riparazione per un'esposizione

Quando si visualizza un risultato di esposizione, il pannello dei dettagli include una scheda Correzioni. Questa scheda elenca i piani di riparazione che risolvono l'esposizione. Un'esposizione può avere più di un piano.

Ogni piano mostra l'azione consigliata, la relativa priorità e la risorsa di destinazione con il relativo tipo di risorsa. Espandi un piano per leggerne le linee guida.

Monitoraggio dell'impatto delle misure correttive sulla dashboard

La dashboard di riepilogo include un widget Piani di riparazione. Il widget elenca fino a cinque piani con lo stato Nuovo o Aggiornato, ordinati per priorità, in modo da poter intervenire sui lavori più urgenti senza aprire l'elenco completo.

Per ogni piano, il widget mostra l'azione consigliata, la priorità del piano, il suo impatto, la risorsa target e Account AWS la risorsa proprietaria. Per vedere le esposizioni alla base di un piano, scegli il suo impatto.

Il widget riporta l'impatto di ogni piano. Non combina l'impatto tra i piani, quindi in ciascuno di questi piani viene conteggiata l'esposizione che più di un piano affronta.

Non puoi applicare filtri a questo widget.

Automazioni in Security Hub

Security Hub include funzionalità che modificano e intervengono automaticamente sui risultati in base alle specifiche dell'utente.

Security Hub attualmente supporta i seguenti tipi di automazioni:

- Regole di automazione: aggiorna e sopprime automaticamente i risultati, nonché invia i risultati agli strumenti di ticketing, quasi in tempo reale in base a criteri definiti.
- Risposta e correzione automatiche: crea EventBridge regole Amazon personalizzate che definiscono le azioni automatiche da intraprendere in base a risultati e approfondimenti specifici.

Le regole di automazione sono utili quando desideri aggiornare automaticamente i campi di ricerca nell'Open Cybersecurity Schema Framework (OCSF). Ad esempio, puoi utilizzare una regola di automazione per aggiornare il livello di gravità dei risultati per le risorse con un tag specifico. L'utilizzo della regola di automazione elimina la necessità di aggiornare manualmente il livello di gravità di ogni risultato correlato al tag specifico. Puoi configurare le regole di automazione per creare ticket in strumenti come Jira Cloud e ServiceNow quando i risultati corrispondono ad attributi specifici. I ticket vengono creati in base ai risultati non appena arrivano in Security Hub.

EventBridge le regole sono utili quando si desidera intraprendere azioni al di fuori di Security Hub per ottenere risultati specifici o inviare risultati specifici a strumenti di terze parti per la correzione o ulteriori indagini. Le regole possono essere utilizzate per attivare azioni supportate, come richiamare una AWS Lambda funzione o notificare a un argomento di Amazon Simple Notification Service (Amazon SNS) un risultato specifico.

Le regole di automazione entrano in vigore prima dell' EventBridge applicazione delle regole. In altre parole, le regole di automazione vengono attivate e aggiornano un risultato prima di EventBridge riceverlo. EventBridge le regole si applicano quindi al risultato aggiornato.

Regole di automazione in Security Hub

Con Security Hub, puoi automatizzare attività come l'aggiornamento dei dettagli dei risultati, l'aggiornamento della criticità delle tue risorse e la creazione di ticket per integrazioni di terze parti.

Regole di automazione e Regioni AWS

Le regole di automazione possono essere create in un'unica Regione AWS soluzione e quindi applicate in tutte le configurazioni Regioni AWS. Quando si utilizza l'aggregazione delle regioni, è possibile creare regole solo nella regione di origine. Quando si creano regole nella regione d'origine, qualsiasi regola definita viene applicata a tutte le regioni collegate, a meno che i criteri della regola non escludano una regione collegata specifica. È necessario creare una regola di automazione per qualsiasi regione che non sia una regione collegata.

Tipi di regole di automazione

Le regole di automazione in Security Hub supportano due tipi di regole: regole di ricerca e regole di risorse. Una regola di ricerca abbina i risultati e aggiorna i dettagli della ricerca o crea un ticket per un'integrazione di terze parti. Una regola relativa alle risorse abbina le risorse e stabilisce la criticità di tali risorse. Una singola regola utilizza criteri di ricerca o criteri relativi alle risorse, ma non entrambi. Una regola relativa alle risorse associa i criteri delle risorse all'azione relativa alla risorsa per impostare la criticità e non può aggiornare i dettagli della ricerca o creare un ticket.

Le regole di ricerca e le regole delle risorse condividono la stessa quota. Puoi creare un massimo di 100 regole di automazione per account per account Regione AWS, sia per le regole di ricerca che per le regole delle risorse.

Individuazione delle azioni e dei criteri relativi alle regole

Le regole di automazione in Security Hub utilizzano criteri per fare riferimento agli attributi OCSF nei risultati di Security Hub. Ad esempio, i filtri supportati per il `Criteria` parametro in CreateAutomationRuleV2corrispondono ai filtri supportati per il `Filters` parametro in GetFindings V2. Ciò significa che i filtri utilizzati nelle regole di automazione possono essere utilizzati per ottenere risultati. Security Hub supporta i seguenti campi OCSF per i criteri delle regole di automazione.

Campo OCSF	Valore del filtro della console	Operatori di filtro	Tipo di campo
`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,`	`String`

Campo OCSF	Valore del filtro della console	Operatori di filtro	Tipo di campo
		NOT_EQUALS, PREFIX_NOT_EQUALS	
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

Campo OCSF	Valore del filtro della console	Operatori di filtro	Tipo di campo
compliance.assessments.meets_criteria	Compliance assessment meets criteria	True, False	Boolean
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

Campo OCSF	Valore del filtro della console	Operatori di filtro	Tipo di campo
compliance.status_id	Compliance status ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
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)

Campo OCSF	Valore del filtro della console	Operatori di filtro	Tipo di campo
finding_info.modified_time_dt	Updated at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
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

Campo OCSF	Valore del filtro della console	Operatori di filtro	Tipo di campo
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

Campo OCSF	Valore del filtro della console	Operatori di filtro	Tipo di campo
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

Campo OCSF	Valore del filtro della console	Operatori di filtro	Tipo di campo
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

Campo OCSF	Valore del filtro della console	Operatori di filtro	Tipo di campo
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

Campo OCSF	Valore del filtro della console	Operatori di filtro	Tipo di campo
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

Campo OCSF	Valore del filtro della console	Operatori di filtro	Tipo di campo
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

Per i criteri etichettati come campi stringa, l'utilizzo di operatori di filtro diversi sullo stesso campo influisce sulla logica di valutazione. Per ulteriori informazioni, consulta il riferimento StringFilterall'API Security Hub.

Ogni criterio supporta un numero massimo di valori che possono essere utilizzati per filtrare i risultati corrispondenti. Per i limiti di ogni criterio, vedere il riferimento OcsfFindingFiltersall'API Security Hub

Campi OCSF che possono essere aggiornati

Di seguito sono riportati i campi OCSF che possono essere aggiornati utilizzando le regole di automazione.

- `Comment`
- `SeverityId`
- `StatusId`

Azioni e criteri relativi alle regole delle risorse

I criteri delle risorse fanno riferimento agli attributi delle risorse. I filtri supportati per i criteri delle risorse sono un sottoinsieme dei filtri supportati per l'operazione GetResourcesV2. È possibile combinare filtri con `OR` operatori `AND` e annidarli fino a tre livelli di profondità, con un massimo di 100 filtri per regola.

Security Hub supporta i seguenti campi di risorse per i criteri delle risorse.

Campo delle risorse	Valore del filtro della console	Operatori di filtro	Tipo di campo
`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`
`ResourceType`	`Resource type`	`EQUALS, PREFIX, CONTAINS, NOT_CONTA`	`String`

Campo delle risorse	Valore del filtro della console	Operatori di filtro	Tipo di campo
		INS, NOT_EQUALS, PREFIX_NOT_EQUALS	
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

Campo delle risorse	Valore del filtro della console	Operatori di filtro	Tipo di campo
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

Campo delle risorse	Valore del filtro della console	Operatori di filtro	Tipo di campo
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 non supporta i filtri numerici. Non supporta l'CONTAINS_WORDoperatore per i criteri relativi alle risorse. Per l'elenco completo dei campi di filtro delle risorse e dei relativi valori consentiti, vedere ResourcesFilterse GetResourcesV2 nel riferimento all'API Security Hub.

Campi di risorse che possono essere aggiornati

Una regola relativa alle risorse aggiorna la criticità delle risorse che corrispondono ai criteri specificati. È possibile impostare la criticità su uno dei seguenti valori, elencati dal più alto al più basso.

- `Very High`
- `High`
- `Medium`
- `Low`
- `Unknown`

Le regole relative alle risorse non si applicano alle risorse AI ospitate autonomamente. Questi tipi di risorse sono esclusi dalla criticità delle regole di automazione e continuano a ricevere una criticità dedotta.

In che modo le regole di automazione valutano i risultati

Una regola di automazione valuta i risultati nuovi e aggiornati generati o acquisiti da Security Hub dopo la creazione della regola.

Le regole di automazione valutano i risultati originali forniti dal provider. I provider possono fornire nuovi risultati e aggiornare i risultati esistenti attraverso la loro integrazione con Security Hub. Le regole non vengono attivate quando si aggiornano i campi di ricerca dopo la creazione delle regole tramite l'`BatchUpdateFindingsV2`operazione. Se si crea una regola di automazione e si effettua un `BatchUpdateFindingsV2` aggiornamento che influiscono entrambi sullo stesso campo di ricerca, l'ultimo aggiornamento imposta il valore per quel campo. Prendiamo l'esempio seguente:

Si usa `BatchUpdateFindingsV2` per aggiornare il `Status` campo di un risultato da `New` a`In Process`. Se chiami`GetFindingsV2`, il `Status` campo ora ha un valore di`In Process`. Crei una regola di automazione che modifica il `Status` campo del risultato da `New` a `Suppressed` (ricorda che le regole ignorano gli aggiornamenti effettuati con`BatchUpdateFindingsV2`). Il provider di ricerca aggiorna il risultato e modifica il `Status` campo in`New`. Se si chiama`GetFindingsV2`, il `Status` campo ora ha un valore pari a `Suppressed` perché è stata applicata la regola di automazione e la regola è stata l'ultima azione intrapresa sul risultato.

Quando si crea o si modifica una regola sulla console Security Hub, la console mostra un'anteprima dei risultati che corrispondono ai criteri della regola. Mentre le regole di automazione valutano i risultati originali inviati dal provider dei risultati, l'anteprima della console riflette i risultati nel loro stato finale così come verrebbero visualizzati in risposta all'operazione dell'`GetFindingsV2`API (ovvero, dopo l'applicazione delle azioni delle regole o di altri aggiornamenti al risultato).

Come vengono ordinate le regole di automazione

A ogni regola di automazione viene assegnato un ordine di regole. Ciò determina l'ordine in cui Security Hub applica le regole di automazione e diventa importante quando più regole si riferiscono allo stesso campo di ricerca o ricerca.

Quando più azioni delle regole si riferiscono allo stesso campo di ricerca o di ricerca, la regola con il valore numerico più alto per l'ordine delle regole si applica per ultima e ha l'effetto finale.

L'ordine delle regole determina anche la criticità finale di una risorsa. Quando più regole relative alle risorse corrispondono alla stessa risorsa, la regola applicata per ultima determina la criticità della risorsa.

Quando si crea una regola nella console di Security Hub, Security Hub assegna automaticamente l'ordine delle regole in base all'ordine di creazione delle regole. La prima regola creata avrà un ordine di regole pari a 1. Se esistono più regole, ogni regola creata successivamente avrà il valore numerico immediatamente più alto disponibile per l'ordine delle regole.

Quando crei una regola tramite CreateAutomationRuleV2API o AWS CLI, Security Hub applica per `RuleOrder` prima la regola con il valore numerico più basso. Quindi applica le regole successive in ordine crescente. Se più risultati sono ugualiRuleOrder, Security Hub applica prima una regola con un valore precedente per il `UpdatedAt` campo (ovvero, la regola che è stata modificata più di recente si applica per ultima).

È possibile modificare l'ordine delle regole in qualsiasi momento.

Esempio di ordine delle regole:

Regola A (l'ordine delle regole è**1**):

- Criteri della regola A
  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type` è `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` è `NEW`
  - `Workflow.Status` = `ACTIVE`
- Azioni della regola A
  - Aggiorna `Confidence` a `95`
  - Aggiorna `Severity` a `CRITICAL`

- Aggiorna `Comment` a `This needs attention`

Regola B (l'ordine delle regole è**2**):

- Criteri della regola B
  - `AwsAccountId` = `123456789012`
- Azioni della regola B
  - Aggiorna `Severity` a `INFORMATIONAL`

Innanzitutto, le azioni della Regola A si applicano ai risultati del Security Hub che soddisfano i criteri della Regola A. Quindi, le azioni della Regola B si applicano ai risultati del Security Hub con l'ID account specificato. In questo esempio, poiché la regola B si applica per ultima, il valore finale dei `Severity` risultati derivanti dall'ID account specificato è`INFORMATIONAL`. In base all'azione della Regola A, il valore finale dei `Confidence` risultati corrispondenti è`95`.

Third-party integrazioni

Puoi utilizzare le regole di automazione per creare ticket per le integrazioni con Jira Cloud e. ServiceNow ITSM Per ulteriori informazioni, consulta Creazione di una regola per un'integrazione di terze parti.

Scenari in cui le regole di automazione non funzionano

Di seguito sono riportati gli scenari in cui le regole di automazione non funzionano.

- L'account autonomo diventa membro di un'organizzazione con un amministratore delegato
- L'account di gestione dell'organizzazione rimuove l'amministratore delegato e ne imposta un nuovo amministratore delegato
- La configurazione dell'aggregatore per l'amministratore delegato o l'account autonomo cambia quando una regione non collegata diventa una regione collegata

In questi scenari, un membro di un'organizzazione può gestire le regole di automazione con le operazioni di elenco, acquisizione ed eliminazione nelle API o. AWS CLI

Quando una regione non collegata diventa una regione collegata, l'amministratore delegato o l'account autonomo può gestire le risorse in una regione collegata con operazioni di elenco, acquisizione ed eliminazione.

Creazione di regole di automazione in Security Hub

Questo argomento descrive come creare regole di automazione. Puoi utilizzare le regole di automazione per aggiornare i dettagli di un risultato, aggiornare la criticità delle tue risorse o creare un ticket per un'integrazione di terze parti. È necessario creare le regole di automazione singolarmente e nel Regione AWS luogo in cui si desidera che vengano applicate. Tuttavia, se si crea una regola di automazione in una regione di aggregazione, questa viene applicata in tutte le regioni. Altrimenti, se si crea una regola di automazione in una regione non collegata, questa viene applicata solo in quella regione.

Creazione di una regola che aggiorni i dettagli della ricerca

La procedura seguente descrive come creare una regola che aggiorni i dettagli dei risultati.

1. Accedi al tuo AWS account. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal riquadro di navigazione, in Gestione, scegli Automazioni.
3. Scegli Crea regola.
4. In Dettagli, inserisci un nome per la regola di automazione.
   - (Facoltativo) Inserisci una descrizione per la regola di automazione.
5. In Azioni, scegli Aggiorna i dettagli dei risultati. Puoi cercare criteri e aggiungere criteri nella barra di ricerca. Per verificare se alcuni risultati corrispondono ai tuoi criteri, scegli Anteprima dei risultati corrispondenti.
6. In Aggiorna i dettagli dei risultati, scegli almeno un dettaglio di ricerca da aggiornare quando un risultato corrisponde ai tuoi criteri. Puoi scegliere Severità, Stato o Commento.
7. In Impostazioni delle regole, seleziona Abilitato o Disabilitato. Se selezioni Abilitato, la regola di automazione viene abilitata ed elabora i nuovi risultati. Se si seleziona Disabilitato, la regola di automazione viene disabilitata e non elabora alcun risultato.
8. (Facoltativo) In Tag, scegli Aggiungi nuovo tag per inserire una coppia chiave-valore da applicare alla regola di automazione.
9. Scegli Crea regola.

Creazione di una regola che aggiorni la criticità delle risorse

La procedura seguente descrive come creare una regola che aggiorni la criticità delle risorse che soddisfano i criteri specificati.

1. Accedi al tuo AWS account. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal riquadro di navigazione, in Gestione, scegli Automazioni.
3. Scegli Crea regola.
4. In Dettagli, inserisci un nome per la regola di automazione.
   - (Facoltativo) Inserisci una descrizione per la regola di automazione.
5. In Azioni, scegli Aggiorna i dettagli delle risorse. Puoi cercare criteri e aggiungere criteri nella barra di ricerca. Per verificare se alcune risorse corrispondono ai tuoi criteri, scegli Anteprima delle risorse corrispondenti.
6. In Aggiorna i dettagli delle risorse, in Criticità, scegli la criticità da applicare alle risorse che corrispondono ai tuoi criteri. Puoi scegliere Molto alta, Alta, Media, Bassa o Sconosciuta.

   > **Note**
   >
   > Questa regola non si applica alle risorse AI ospitate autonomamente. Questi tipi di risorse sono esclusi dalla criticità delle regole di automazione.

7. In Impostazioni delle regole, seleziona Abilitato o Disabilitato. Se selezioni Abilitato, la regola di automazione viene abilitata ed elabora le risorse che soddisfano i criteri specificati. Se si seleziona Disabilitato, la regola di automazione viene disabilitata e non elabora alcuna risorsa.
8. (Facoltativo) In Tag, scegli Aggiungi nuovo tag per inserire una coppia chiave-valore da applicare alla regola di automazione.
9. Scegli Crea regola.

Creazione di una regola per un'integrazione di terze parti

La procedura seguente descrive come creare una regola che crei un ticket per un'integrazione di terze parti. Per informazioni sulle integrazioni supportate da Security Hub CSPM, vedi Third-party integrazioni per Security Hub CSPM.

1. Accedi al tuo account. AWS Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal riquadro di navigazione, in Gestione, scegli Automazioni.
3. Scegli Crea regola.
4. In Dettagli, inserisci un nome per la regola di automazione.

- (Facoltativo) Inserisci una descrizione per la regola di automazione.

5. In Azioni, scegli Crea ticket. Puoi cercare criteri e aggiungere criteri nella barra di ricerca. Per verificare se alcuni risultati corrispondono ai tuoi criteri, scegli Anteprima dei risultati corrispondenti.
6. In Crea un ticket, scegli un'integrazione di ticketing IT dal menu a discesa, quindi scegli Aggiungi integrazione.
7. In Impostazioni delle regole, seleziona Abilitato o Disabilitato. Se selezioni Abilitato, la regola di automazione viene abilitata ed elabora i nuovi risultati. Se si seleziona Disabilitato, la regola di automazione viene disabilitata e non elabora alcun risultato.
8. (Facoltativo) In Tag, scegli Aggiungi nuovo tag per inserire una coppia chiave-valore da applicare alla regola di automazione.
9. Scegli Crea regola.

Visualizzazione dei dettagli delle regole di automazione in Security Hub

Questo argomento descrive come visualizzare i dettagli delle regole di automazione. È possibile visualizzare i seguenti dettagli per una regola di automazione:

- Nome e descrizione
- Azioni e criteri
- Stato delle regole e risultati esistenti
- Tag

Per visualizzare i dettagli di una regola di automazione

1. Accedi al tuo AWS account. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal pannello di navigazione, in Gestione, scegli Automazioni. Questa schermata mostra tutte le regole di automazione create.
3. Seleziona la regola di automazione che desideri visualizzare. Seleziona Visualizza dettagli. In alternativa, puoi scegliere il nome della regola di automazione che desideri visualizzare.

Aggiornamento dell'ordine delle regole in Security Hub

Questo argomento descrive come aggiornare l'ordine delle regole di automazione nella console. Se desideri modificare i criteri per una regola di automazione, vedi Modifica delle regole di automazione in Security Hub.

Non è possibile aggiornare l'ordine delle regole per una regola di automazione senza aggiornare l'ordine delle regole per ogni regola di automazione. Ad esempio, hai quattro regole di automazione: Regola A (1), Regola B (2), Regola C (3) e Regola D (4). Vuoi che la regola D venga applicata per prima. Per fare ciò, ne modifichi il numero da 4 a 1. Di conseguenza, la regola A ottiene 2, la regola B ottiene 3 e la regola C ottiene 4.

Per aggiornare l'ordine delle regole di automazione

1. Accedi al tuo AWS account. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal pannello di navigazione, in Gestione, scegli Automazioni.
3. Seleziona la regola di automazione che desideri modificare. In Ordine, scegli l'icona a forma di matita accanto al numero dell'ordine. Utilizza le frecce per determinare il nuovo numero d'ordine. Scegli l'icona ✓ per confermare. Scegli l'icona X per annullare. In alternativa, puoi scegliere Cambia ordine per spostare la regola di automazione verso il basso, verso l'alto o in cima all'elenco.

Disattivazione delle regole di automazione in Security Hub

Questo argomento descrive come disattivare le regole di automazione. Quando si disattivano le regole di automazione, Security Hub smette di applicarle. Puoi disabilitare le regole di automazione in qualsiasi momento e nel Regione AWS luogo in cui le hai create.

Per disattivare una regola

1. Accedi al tuo AWS account. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal pannello di navigazione, in Gestione, scegli Automazioni.
3. Seleziona la regola di automazione che desideri disattivare. In Stato, scegli l'icona a forma di matita accanto a Abilitato. Scegli il menu a discesa, quindi scegli Disabilitato. Scegli l'icona ✓ per confermare. Scegli l'icona X per annullare. Puoi anche scegliere Disabilita dal menu a discesa Azioni.

Abilitazione di una regola di automazione in Security Hub

Questo argomento descrive come abilitare le regole di automazione. Quando si abilitano le regole di automazione, Security Hub riprende ad applicarle. Puoi abilitare le regole di automazione in qualsiasi momento e nel luogo in Regione AWS cui le hai create.

Per abilitare una regola

1. Accedi al tuo AWS account. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal pannello di navigazione, in Gestione, scegli Automazioni.
3. Seleziona la regola di automazione che desideri abilitare. In Stato, scegli l'icona a forma di matita accanto a Disabilitato. Scegli il menu a discesa, quindi scegli Abilitato. Scegli l'icona ✓ per confermare. Scegli l'icona X per annullare. Puoi anche scegliere Abilita dal menu a discesa Azioni.

Duplicazione delle regole di automazione in Security Hub

Questo argomento descrive come duplicare le regole di automazione. La duplicazione delle regole di automazione può aiutarti a risparmiare tempo se vuoi evitare di crearle da zero. Quando duplichi le regole di automazione, puoi aggiornare dettagli, azioni, impostazioni delle regole e tag. Puoi modificare le regole di automazione nel luogo in Regione AWS cui le hai create.

Per duplicare una regola

1. Accedi al tuo AWS account e apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal pannello di navigazione, scegli Gestione e scegli Automazioni.
3. Seleziona la regola di automazione che desideri duplicare. Quindi scegli Azioni, quindi scegli Duplica.
4. Apporta e rivedi le modifiche, quindi scegli Crea regola.

Modifica delle regole di automazione in Security Hub

Questo argomento descrive come modificare le regole di automazione. È possibile modificare le regole di automazione nel Regione AWS luogo in cui sono state create.

È possibile modificare quanto segue per le regole di automazione:

- Nome e descrizione
- Azioni
- Impostazioni delle regole

Non è possibile modificare i tag per le regole di automazione.

Per modificare una regola

1. Accedi al tuo AWS account. Apri la console Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal pannello di navigazione, in Gestione, scegli Automazioni.
3. Seleziona la regola di automazione che desideri modificare. Seleziona Azioni, quindi scegli Modifica.
4. Apporta e rivedi le tue modifiche.
5. Scegli Save changes (Salva modifiche).

Eliminazione delle regole di automazione in Security Hub

Questo argomento descrive come eliminare le regole di automazione. È possibile eliminare le regole di automazione nel Regione AWS luogo in cui sono state create.

Come eliminare una regola

1. Accedi al tuo AWS account e apri la console di Security Hub all'indirizzo https://console.aws.amazon.com/securityhub/v2/home.
2. Dal pannello di navigazione, scegli Gestione, quindi scegli Automazioni.
3. Seleziona la regola di automazione che desideri eliminare. Scegli Azioni, quindi Elimina.
4. Scegli Delete (Elimina).

Regole di automazione in EventBridge

Puoi utilizzare le regole di automazione in Amazon EventBridge per rispondere ai risultati di Security Hub. Security Hub invia i risultati EventBridge come eventi quasi in tempo reale. Puoi scrivere regole di base che indicano quali azioni automatiche intraprendere quando un evento corrisponde a una regola. Le azioni che possono essere attivate automaticamente includono quanto segue:

- Configurazione di una destinazione API in. EventBridge
- Richiamo dei comandi di esecuzione di Amazon EC2
- Richiamo di funzioni Lambda
- Richiamo delle macchine a stati Step Functions
- Notifica di un argomento Amazon SNS o di una coda Amazon SQS
- Inoltro di eventi a Kinesis Data Streams
- Invio di una ricerca a uno strumento di gestione di ticket, chat, SIEM o risposta agli incidenti di terze parti
- Invio di un evento a un EventBridge bus in un altro account AWS

Security Hub invia nuovi risultati e risultati aggiornati a EventBridge come eventi. Quindi si configurano EventBridge le regole per rispondere a ciascun evento di Security Hub. Per ulteriori informazioni, vedi Che cos'è EventBridge? nella Guida EventBridge per l'utente.

> **Note**
>
> Se hai definito EventBridge delle regole per i risultati in Security Hub CSPM, le regole potrebbero sovrapporsi alle regole definite per Security Hub. Per evitare l'invio di risultati duplicati, valuta le regole che hai definito per Security Hub CSPM per determinare se si sovrappongono alle regole che hai definito per Security Hub. Ove applicabile, disabilita le regole CSPM di Security Hub sostituite dalle regole di Security Hub.

> **Note**
>
> Come procedura consigliata, assicurati che gli utenti con autorizzazione all'accesso EventBridge utilizzino AWS Identity and Access Management politiche che concedano le autorizzazioni minime richieste. Per ulteriori informazioni, consulta EventBridge e AWS Identity and Access Management nella Guida per l'EventBridge utente.

EventBridge tipi di eventi

Security Hub utilizza i seguenti tipi di EventBridge eventi Amazon per l'integrazione con EventBridge.

Nella EventBridge dashboard di Security Hub, All Events include tutti questi tipi di eventi.

Risultati importati (V2)

Security Hub invia automaticamente tutti i nuovi risultati e tutti gli aggiornamenti ai risultati esistenti EventBridge come Findings Imported V2 eventi. Ogni Findings Imported V2 evento contiene un singolo risultato.

Ogni risultato importato e ogni risultato aggiornato tramite una `BatchUpdateFindingsV2` richiesta attiva un Findings Imported V2 evento.

Per gli account amministratore, il feed degli eventi EventBridge include eventi relativi ai risultati relativi all'account e agli account dei membri.

In una regione di aggregazione, il feed degli eventi include gli eventi relativi ai risultati della regione di aggregazione e delle regioni collegate. Cross-Region i risultati sono inclusi nel feed degli eventi quasi in tempo reale.

È possibile definire regole EventBridge che indirizzino automaticamente i risultati a un flusso di lavoro di correzione, a uno strumento di terze parti o a un altro EventBridge obiettivo supportato. Le regole possono includere filtri che applicano la regola solo se il risultato ha valori di attributo specifici.

Si utilizza questo metodo per inviare automaticamente tutti i risultati, o tutti i risultati con caratteristiche specifiche, a un flusso di lavoro di risposta o correzione.

> **Note**
>
> Security Hub e Security Hub CSPM inviano entrambi i risultati a EventBridge sotto la fonte di. `aws.securityhub` Assicurati che EventBridge le tue regole utilizzino il tipo di dettaglio specifico di Security Hub per evitare notifiche duplicate relative ai risultati del CSPM di Security Hub.

EventBridge formati di eventi

Il tipo di Findings Imported V2 evento utilizza il seguente formato di evento.

Esempio

Questo formato viene utilizzato quando Security Hub invia un evento a 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>
       }]
   }
}
```

Ogni evento invia un singolo risultato. *<finding content>*è il contenuto in JSON del risultato inviato dall'evento.

Per un elenco completo degli attributi di ricerca, consulta i risultati OCSF in Security Hub CSPM.

Configurazione delle regole per EventBridge

Puoi creare una regola in Amazon EventBridge che definisce un'azione da intraprendere quando viene ricevuto un Findings Imported V2 evento. Findings Imported V2gli eventi vengono attivati dagli aggiornamenti tramite `BatchUpdateFindingsV2`.

Ogni regola contiene un pattern di eventi, che identifica gli eventi che attivano la regola. Il modello di evento contiene sempre l'origine dell'evento (`aws.securityhub`) e il tipo di evento (Findings Imported V2). Il pattern di eventi può anche specificare filtri per identificare i risultati a cui si applica la regola.

La regola dell'evento identifica quindi gli obiettivi della regola. Gli obiettivi sono le azioni da intraprendere quando si EventBridge riceve un evento Findings Imported V2 e il risultato corrisponde ai filtri.

Le istruzioni fornite qui utilizzano la EventBridge console. Quando usi la console, crea EventBridge automaticamente la policy richiesta basata sulle risorse che consente di EventBridge scrivere su Amazon Logs. CloudWatch

Puoi anche utilizzare il `PutRule` funzionamento dell'API. EventBridge Tuttavia, se si utilizza l' EventBridge API, è necessario creare la policy basata sulle risorse. Per informazioni sulla policy richiesta, consulta le autorizzazioni CloudWatch dei log nella Amazon User Guide. EventBridge

Formato del modello di evento

Il formato del modello di evento per gli eventi Findings Imported V2 è il seguente:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Findings Imported V2"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`identifica Security Hub come servizio che genera l'evento.
- `detail-type`identifica il tipo di evento.
- `detail`è facoltativo e fornisce i valori di filtro per il modello di evento. Se il modello di evento non contiene un `detail` campo, tutti i risultati attivano la regola.

Puoi filtrare i risultati in base a qualsiasi attributo di ricerca. Per ogni attributo, fornisci una matrice separata da virgole di uno o più valori.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Se fornisci più di un valore per un attributo, questi valori vengono uniti da. `OR` Un risultato corrisponde al filtro per un singolo attributo se il risultato contiene uno dei valori elencati. Ad esempio, se fornisci entrambi i valori `INFORMATIONAL` e `LOW` come valori per`Severity.Label`, il risultato corrisponde se ha un'etichetta di gravità pari a uno `INFORMATIONAL` o`LOW`.

Gli attributi sono uniti da`AND`. Un risultato corrisponde se corrisponde ai criteri di filtro per tutti gli attributi forniti.

Quando si fornisce un valore di attributo, questo deve riflettere la posizione di tale attributo all'interno della struttura AWS Open Cybersecurity Schema Framework (OCSF).

Nell'esempio seguente, il modello di evento fornisce valori di filtro per `ProductArn` e`Severity.Label`, pertanto, un risultato corrisponde se è generato da Amazon Inspector e ha un'etichetta di gravità pari a o. `INFORMATIONAL` `LOW`

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Findings Imported V2"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

Creazione di una regola di evento

È possibile utilizzare un modello di evento predefinito o un modello di evento personalizzato per creare una regola in EventBridge. Se si seleziona un modello predefinito, compila EventBridge automaticamente e. `source` `detail-type` EventBridge fornisce anche campi per specificare i valori di filtro per i seguenti attributi di ricerca:

- `cloud.account.uid`
- `compliance.status`
- `metadata.product.name`
- `resources.uid`
- `severity`
- `status`

Per creare una EventBridge regola (console)

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Utilizzando i seguenti valori, crea una EventBridge regola che monitora la ricerca degli eventi:

- Per Tipo di regola, scegli Regola con un modello di eventi.
- Scegli come creare lo schema degli eventi.

Per creare il modello dell'evento con...	Esegui questa operazione…	
Un modello	Nella sezione Schema degli eventi, scegli le seguenti opzioni: • Per Origine evento, scegli Servizi AWS . • Per l'AWS assistenza, scegli Security Hub. • Per il tipo di evento, scegli Findings Imported V2. • (Facoltativo) Per rendere la regola più specifica, aggiungi i valori del filtro. Ad esempio, per limitare la regola ai risultati con stati di record attivi, per gli stati di record specifici, scegli Attivo.	

Per creare il modello dell'evento con...	Esegui questa operazione…
Un modello di evento personalizzato (Utilizza uno schema personalizzato se desideri filtrare i risultati in base agli attributi che non vengono visualizzati nella EventBridge console.)	• Nella sezione Schema di eventi, scegli Modelli personalizzati (editor JSON), quindi incolla il seguente modello di evento nell'area di testo: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Findings Imported V2" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>" ] } } }` • Aggiorna il modello di evento per includere l'attributo e i valori degli attributi che desideri utilizzare come filtro. Ad esempio, per applicare la regola ai risultati con una gravità di`Critical`, utilizza il seguente esempio di modello:

Per creare il modello dell'evento con...	Esegui questa operazione…

	<pre>{
	    "source":
	["aws.securityhub"
	],
	    "detail-type":
	["Findings Imported
	 V2"],
	    "detail":{
	        "findings":
	{
	           "Severity
	": ["Critical"]
	          }
	    }
	}</pre>

- Per i tipi di target, scegli il AWS servizio e per Seleziona un target, scegli un obiettivo, ad esempio un argomento o una AWS Lambda funzione di Amazon SNS. La destinazione viene attivata quando viene ricevuto un evento che corrisponde al modello di evento definito nella regola.

Per informazioni dettagliate sulla creazione di regole, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi nella Amazon EventBridge User Guide.

> **Note**
>
> Se hai definito EventBridge delle regole per i risultati in Security Hub CSPM, le regole potrebbero sovrapporsi alle regole definite per Security Hub. Per evitare l'invio di risultati duplicati, valuta le regole che hai definito per Security Hub CSPM per determinare se si sovrappongono alle regole che hai definito per Security Hub. Ove applicabile, disabilita le regole CSPM di Security Hub sostituite dalle regole di Security Hub.

Esportazione dei risultati da Security Hub ad Amazon S3

Puoi esportare i risultati da AWS Security Hub in un bucket Amazon Simple Storage Service (Amazon S3) di tua proprietà. Un'esportazione acquisisce i risultati che corrispondono ai filtri sulla pagina da cui l'hai avviata e li scrive nel tuo bucket come file CSV o come JSON nel formato Open Cybersecurity Schema Framework (OCSF). Utilizza le esportazioni per condividere i risultati con i team che non utilizzano la console Security Hub, caricare i risultati in un data warehouse o in uno strumento di business intelligence o conservare un record temporale per gli audit.

Le esportazioni sono su richiesta. Si avvia un'esportazione, Security Hub la esegue in background e i file vengono visualizzati nel bucket al termine. È possibile tenere traccia di ogni esportazione dalla pagina Esportazioni della console Security Hub.

Come funziona l'esportazione dei risultati

Si avvia un'esportazione da una delle pagine dei risultati nella console di Security Hub: Tutti i risultati, Esposizione, Minacce, Vulnerabilità, Dati sensibili o Gestione della postura. L'esportazione utilizza la pagina come ambito e riprende i filtri applicati in quella pagina. Ad esempio, se si filtra la pagina Vulnerabilità in base ai risultati critici con lo stato`New`, l'esportazione contiene solo tali risultati.

Security Hub scrive l'esportazione nel bucket Amazon S3 e il prefisso che scegli e crittografa ogni oggetto con la chiave AWS Key Management Service ()AWS KMS che scegli.

> **Note**
>
> È possibile eseguire una sola esportazione alla volta in un account. Per iniziare un'altra esportazione, attendi che l'esportazione in corso finisca o annullala dalla pagina Esportazioni.

Prerequisiti

Prima di creare un'esportazione, hai bisogno di un bucket Amazon S3, di una AWS KMS chiave, di policy che consentano a Security Hub di scrivere su di essi e delle autorizzazioni IAM per l'identità che crea l'esportazione.

Creare un'esportazione

Per creare un'esportazione

1. Apri la console Security Hub e scegli la pagina dei risultati da cui desideri esportare: Tutti i risultati, Esposizione, Minacce, Vulnerabilità, Dati sensibili o Gestione della postura.
2. Applica i filtri che desideri utilizzare per l'esportazione.
3. Scegli Export (Esporta). Viene visualizzata la pagina Crea esportazione.
4. In Ambito, esamina l'ambito. Legge Tutti i risultati, utilizzando i filtri riportati dalla pagina Vulnerabilità (o il nome della pagina da cui provieni). Per modificare l'ambito o i filtri, torna alla pagina dei risultati e modificali lì.

   I filtri vengono applicati ai campi OCSF. Se un filtro nella pagina di origine non si applica ai risultati, la console mostra un avviso che indica i filtri che non è stato trasferito.
5. In Impostazioni di esportazione, procedi come segue:

   - Nome di esportazione: inserisci un nome in modo da poter trovare l'esportazione più avanti nell'elenco delle esportazioni. La console suggerisce, ad esempio, un nome creato dalla pagina di origine e dall'ora corrente`vulnerabilities-202610081601`.
   - Formato di esportazione: scegli CSV o JSON (OCSF).
   - Colonne CSV (solo CSV): ogni opzione mostra il nome della colonna e il percorso del campo OCSF da cui proviene, ad esempio Finding account (). `cloud.account.uid` I campi sono raggruppati per oggetto OCSF, ad esempio Finding info, Cloud, Resources, Compliance, Vulnerabilities ed Evidences. Il set predefinito contiene nove colonne: Finding title, Severity, Resource ID, Created at, Status, Finding account, Finding region, Product vendor name e Finding type.

     Le esportazioni JSON (OCSF) contengono sempre i risultati completi, quindi non è prevista alcuna selezione di colonne.
6. In Export location, seleziona il tuo bucket Amazon S3 e aggiungi la AWS KMS chiave per la crittografia.
7. Scegli Crea esportazione.

Se nel tuo account è già in esecuzione un'esportazione, la console mostra la finestra di dialogo Esportazione in corso. Puoi attendere che l'esportazione finisca o scegliere Annulla esportazione e creane una nuova per annullarla e iniziare questa.

Third-party integrazioni per Security Hub

Puoi migliorare il tuo livello di sicurezza con integrazioni di terze parti per AWS Security Hub. Con questa funzionalità puoi abilitare integrazioni che utilizzano i risultati di Security Hub, consentendoti di incorporare i tuoi strumenti operativi, di indagine e di risposta con Security Hub. Attualmente Security Hub supporta l'integrazione con Jira Cloud eServiceNow.

Argomenti

- Integrazioni per AWS Security Hub Jira Cloud
- Integrazioni per ServiceNow
- Politiche chiave KMS per le integrazioni di ticketing di Security Hub
- Test delle integrazioni di ticketing configurate

Integrazioni per AWS Security Hub Jira Cloud

Questo argomento descrive come integrare Security Hub conJira Cloud. Prima di completare una qualsiasi delle procedure descritte in questo argomento, è necessario acquistare un piano di Jira Cloud abbonamento. Per informazioni sui piani di abbonamento, consulta la sezione Prezzi sul Atlassian sito Web.

Questa integrazione ti consente di inviare i risultati del Security Hub a Jira Cloud, manualmente o automaticamente, in modo da poterli gestire come parte dei flussi di lavoro operativi. Ad esempio, puoi assegnare la proprietà ai problemi che richiedono indagini e correzioni.

Per gli account di un'organizzazione, solo l'amministratore delegato può configurare un'integrazione. L'amministratore delegato può utilizzare manualmente la funzione di creazione del ticket per i risultati degli account di qualsiasi membro. Inoltre, l'amministratore delegato può utilizzare le regole di automazione per creare automaticamente ticket per eventuali risultati associati agli account dei membri. Quando definisce una regola di automazione, l'amministratore delegato può impostare criteri, che possono includere tutti gli account membri o account membro specifici. Per informazioni sull'impostazione di un amministratore delegato, vedere Impostazione di un account amministratore delegato in Security Hub.

Per gli account che non appartengono a un'organizzazione, sono disponibili tutti gli aspetti di questa funzionalità.

Prerequisiti

Prima di connettere Security Hub al tuo Jira Cloud ambiente, devi assicurarti che i seguenti passaggi di configurazione vengano eseguiti nel tuo ambiente Jira.

- Installa l'app cloud AWS Security Hub for Jira.
- Avere almeno un progetto di sviluppo software gestito dall'azienda.
- Assegna l' AWS app ai progetti di sviluppo software per i quali desideri ricevere i risultati da Security Hub.

I passaggi per ciascuno di questi prerequisiti sono elencati di seguito.

1. Installa il AWS Security Hub per Jira Cloud app

Security Hub dispone di un'app per supportarne l'integrazione con Jira. Questa app installa campi personalizzati e un tipo di problema personalizzato. Security Hub li utilizza per compilare attributi specifici sui risultati.

1. Accedi al tuo Atlassian sito come amministratore.
2. Scegli Impostazioni e scegli App.
3. Se sei indirizzato alla pagina del marketplace, scegli Trova nuove app. Se sei indirizzato alla pagina delle app, scegli Esplora app, quindi cerca AWS Security Hub per Jira Cloud. Quindi scegli Scaricalo ora.

2. Crea un progetto o verifica i progetti esistenti

Questo passaggio è necessario se non hai creato un progetto. Per informazioni su come creare un progetto, consulta Creare un nuovo progetto nella Jira Cloud Support documentazione.

Requisiti per la creazione di un progetto

Assicurati di fare quanto segue quando crei un nuovo progetto.

- Scegli Sviluppo software per il modello di progetto.
- Scegli Company-managedil tipo di progetto.

Requisiti per i progetti esistenti

Tutti i progetti esistenti nell'ambiente Jira che sono integrati con Security Hub devono essere un tipo di progetto di Company-managed.

3. Aggiungi i tuoi progetti al AWS Security Hub per Jira Cloud app

Affinché Security Hub sia in grado di inviare correttamente i risultati al tuo ambiente Jira, ogni progetto che desideri utilizzare con Security Hub deve essere associato all'Jira Cloudapp AWS Security Hub for. L'associazione di un progetto Jira all'app garantisce che i campi personalizzati necessari per Security Hub siano associati al progetto e possano essere compilati quando Security Hub invia i risultati al progetto.

1. Accedi al tuo Atlassian sito come amministratore.
2. Scegli Impostazioni e scegli App.
3. Dall'elenco delle app, scegli AWS Security Hub for Jira Cloud.
4. Scegli la scheda delle impostazioni del connettore.
5. In Progetti abilitati, scegli Aggiungi progetto Jira.
    a. Dal menu a discesa, scegli Aggiungi tutto o seleziona un progetto. Ripeti questa parte del passaggio se desideri aggiungere più di un progetto, ma non tutti i progetti.
    b. Selezionare Salva.

È possibile verificare quali progetti sono stati installati correttamente dalla scheda Installation Manager. È inoltre possibile verificare le configurazioni di campi, schermate, stati e flussi di lavoro dalla scheda Installation Manager.

Per ulteriori informazioni in meritoJira Cloud, consulta Jira Cloudle risorse sul sito Web. Atlassian

Raccomandazioni

Creazione di un account di sistema dedicato per il tuo ambiente Jira

L'integrazione con Security Hub Jira Cloud utilizza una connessione OAuth associata a un utente specifico all'interno dell'istanza Jira. La creazione di un account di sistema dedicato da utilizzare per la connessione Security Hub OAuth è consigliata per la connessione per i seguenti motivi:

- Un utente di sistema dedicato garantisce che la connessione non sia associata a un dipendente le cui autorizzazioni all'ambiente Jira potrebbero cambiare nel tempo, influendo sulla capacità di Security Hub di integrarsi con il tuo ambiente Jira.

- Ogni problema creato da Security Hub in Jira mostra un campo Created By contenente il nome utente utilizzato per creare la connessione OAuth. L'utilizzo di un account di sistema per la connessione OAuth fa sì che questo account di sistema appaia come creatore del ticket, contribuendo a rendere visibile che il risultato è stato creato tramite l'integrazione del Security Hub e non manualmente da un altro utente Jira.

Configurare un'integrazione tra Security Hub e Jira Cloud

La seguente procedura deve essere completata per ciascuno dei Jira Cloud progetti a cui desideri inviare i risultati del Security Hub.

> **Note**
>
> Quando si crea un Jira Cloud connettore, si viene reindirizzati dall'attuale Regione AWS a`"https://3rdp.oauth.console.api.aws"`, in modo da poter completare la registrazione del connettore. Successivamente, si torna al Regione AWS punto in cui è stato creato il connettore.

Per configurare un'integrazione per Jira Cloud

1. Accedi al tuo AWS account con le tue credenziali e apri la console Security Hub all'indirizzohttps://console.aws.amazon.com/securityhub/v2/home? region=us-east-1.
2. Dal riquadro di navigazione, scegli Gestione, quindi scegli Integrazioni.
3. Scegliere AggiungiJira Cloud.
4. Per i dettagli, inserisci un nome univoco e descrittivo per l'integrazione e determina se inserire una descrizione facoltativa per l'integrazione.
5. Per Encryptions, scegli come crittografare le tue credenziali di integrazione all'interno di Security Hub.
   - Usa chiave AWS proprietaria: con questa opzione, viene utilizzata una chiave di servizio di proprietà di Security Hub per crittografare i dati delle credenziali di integrazione all'interno di Security Hub.
   - Scegli una chiave KMS diversa (avanzata): con questa opzione scegli una chiave che hai creato e AWS KMS key che desideri utilizzare per crittografare i dati delle credenziali di integrazione all'interno di Security Hub. Per informazioni su come creare una AWS KMS

chiave, consulta Create a AWS KMS key nella Developer Guide. AWS Key Management Service Se scegli di utilizzare la tua chiave, devi aggiungere dichiarazioni politiche alla chiave KMS che consentano l'accesso al Security Hub alla chiave. Consulta le politiche AWS KMS chiave per le integrazioni dei ticket di Security Hub per i dettagli sulle politiche necessarie.

> **Note**
>
> Non è possibile modificare queste impostazioni una volta completata questa configurazione. Tuttavia, se si sceglie Chiave personalizzata, è possibile modificare la politica relativa alle chiavi personalizzate in qualsiasi momento.

6. (Facoltativo) Per i tag, crea e aggiungi un tag alla tua integrazione. Puoi aggiungere fino a 50 tag.
7. Per le autorizzazioni, scegli Crea connettore e autorizza. Viene visualizzato un pop-up in cui scegli Consenti per completare l'autorizzazione. Dopo aver completato l'autorizzazione, viene visualizzata una casella di controllo che indica che l'autorizzazione è avvenuta con successo.
8. Per Configurazioni, inserisci l'ID del Jira Cloud progetto.
9. Scegli Configurazione completa. Dopo aver completato la configurazione, puoi visualizzare le integrazioni configurate nella scheda Integrazioni configurate.

Dopo aver configurato l'integrazione con Jira, puoi testare la connessione per confermare che tutto sia configurato correttamente nel tuo ambiente Jira e in Security Hub. Per ulteriori informazioni, consulta Testare le integrazioni di ticketing configurate.

Dettagli aggiuntivi sull'integrazione con Jira

Considerazioni sui limiti di velocità

Jira applica i limiti di velocità delle API per mantenere la stabilità del servizio e garantire un utilizzo equo su tutta la piattaforma. Quando si utilizza l'integrazione AWS di Security Hub con Jira, questi limiti di velocità possono influire sull'elaborazione dei risultati di Security Hub, in particolare in ambienti che generano volumi elevati di risultati. Ciò può comportare un ritardo nella creazione dei ticket e, in scenari con volumi di ricerca estremamente elevati, alcuni risultati potrebbero non essere affatto elaborati in ticket Jira. Per ottimizzare la tua integrazione, prendi in considerazione l'implementazione di filtri sulle regole di automazione in Security Hub per dare priorità al ticketing in base ai risultati più importanti, il monitoraggio dell'utilizzo dell'API Jira tramite la loro console di

amministrazione e la pianificazione del flusso di lavoro in base ai limiti di tariffa specifici del tuo livello di licenza Jira. Per le implementazioni aziendali critiche, contatta l'amministratore di Jira per rivedere le allocazioni dei limiti di velocità.

Per informazioni dettagliate sui limiti di velocità delle API Jira, consulta la documentazione relativa alla limitazione della velocità sul sito Web dell'Atlassian Developers Guide.

Autenticazione e sicurezza

L'autenticazione dell'API Jira richiede una corretta configurazione OAuth 2.0 per un accesso sicuro. Assicurati che la tua applicazione segua le migliori pratiche di sicurezza di Atlassian per l'integrazione delle API.

Risorse:

- Jira REST API v3: documentazione di Jira REST API v3 sul sito web di Atlassian
- Implementazione di OAuth 2.0 (3LO): guida all'implementazione di OAuth 2.0 (3LO) sul sito web di Atlassian
- Amministra le app Jira Cloud: risorse di amministrazione di Jira Cloud sul sito web di Atlassian
- Gestisci le autorizzazioni Jira: gestisci le autorizzazioni del progetto sul sito web di Atlassian

Creare un ticket per un Jira Cloud integrazione

Dopo aver creato un'integrazione conJira Cloud, puoi creare un ticket per una scoperta.

> **Note**
>
> Un reperto sarà sempre associato a un singolo ticket durante l'intero ciclo di vita. Security Hub invia tutti gli aggiornamenti successivi a un risultato dello stesso ticket dopo la creazione iniziale. Se un connettore associato a una regola di automazione viene modificato, il connettore aggiornato viene utilizzato solo per i risultati nuovi e in arrivo che soddisfano i criteri della regola.

Per creare un ticket per una scoperta

1. Accedi al tuo AWS account con le tue credenziali e apri la console Security Hub all'indirizzohttps://console.aws.amazon.com/securityhub/v2/home? region=us-east-1.

2. Dal pannello di navigazione, in Inventario, scegli Risultati.
3. Scegli un risultato. Nella ricerca, scegli Crea biglietto.
4. Per l'integrazione, apri il menu a discesa e scegli un'integrazione. Questa integrazione è l'integrazione che hai creato in precedenza quando hai configurato il Jira Cloud progetto. Scegli l'integrazione a cui desideri inviare i risultati.
5. Scegli Crea.

Visualizzazione di un ticket per un Jira Cloud integrazione

Dopo aver creato un ticket per una ricerca, puoi aprirlo sulla tua Jira Cloud istanza.

Per visualizzare un risultato sul tuo Jira Cloud istanza

1. Accedi al tuo AWS account con le tue credenziali e apri la console Security Hub all'indirizzohttps://console.aws.amazon.com/securityhub/v2/home? region=us-east-1.
2. Dal pannello di navigazione, in Inventario, scegli Risultati.
3. Scegli il risultato in cui hai creato il ticket.
4. Nella ricerca, scegli l'ID del ticket per visualizzare il ticket sulla tua Jira Cloud istanza o Visualizza JSON.

Integrazioni per ServiceNow

Questo argomento descrive come accedere alla console Security Hub per configurare un'integrazioneServiceNow ITSM. Prima di completare una qualsiasi delle procedure descritte in questo argomento, è necessario disporre di un abbonamento ServiceNow ITSM prima di poter aggiungere questa integrazione. Per ulteriori informazioni, consulta la pagina dei prezzi sul ServiceNow sito Web.

Per gli account di un'organizzazione, solo l'amministratore delegato può configurare un'integrazione. L'amministratore delegato può utilizzare manualmente la funzione di creazione del ticket per i risultati degli account di qualsiasi membro. Inoltre, l'amministratore delegato può utilizzare le regole di automazione per creare automaticamente ticket per eventuali risultati associati agli account dei membri. Quando definisce una regola di automazione, l'amministratore delegato può impostare criteri, che possono includere tutti gli account membri o account membro specifici. Per informazioni sull'impostazione di un amministratore delegato, vedere Impostazione di un account amministratore delegato in Security Hub.

Per gli account che non appartengono a un'organizzazione, sono disponibili tutti gli aspetti di questa funzionalità.

Prerequisiti: configurare l'ambiente ServiceNow

È necessario completare i seguenti prerequisiti prima di configurare un'integrazione per. ServiceNow ITSM In caso contrario, l'integrazione tra ServiceNow ITSM e Security Hub non funzionerà.

1. Installa l'integrazione di Security Hubfindings per IT Service Management (ITSM)

La procedura seguente descrive come installare il plug-in Security Hub.

1. Accedi all'ServiceNow ITSMistanza, quindi apri il navigatore dell'applicazione.
2. Vai allo ServiceNow Store.
3. Cerca Security Hub trova l'integrazione per IT Service Management (ITSM), quindi scegli Ottieni per installare l'applicazione.

> **Note**
>
> Nelle impostazioni dell'applicazione Security Hub, scegli l'azione da intraprendere quando i nuovi risultati di Security Hub vengono inviati al tuo ServiceNow ITSM ambiente. Puoi scegliere Non fare nulla, Crea incidente, Crea problema o Crea entrambi (incident/problem).

2. Configura il tipo di concessione Client Credentials per le richieste OAuth in entrata

È necessario configurare questo tipo di concessione per le richieste OAuth in entrata. Per ulteriori informazioni, consulta Client Credentials Il tipo di concessione per Inbound OAuth è supportato nella pagina Web Support. ServiceNow

3. Crea un'applicazione OAuth

Se hai già creato un'applicazione OAuth, puoi ignorare questo prerequisito. Per informazioni sulla creazione di un'applicazione OAuth, consulta Configurazione di OAuth sul sito Web. ServiceNow

Prerequisiti: configura AWS Secrets Manager

Per utilizzare l'integrazione di Security Hub con ServiceNow, le credenziali dell'applicazione ServiceNow OAuth devono essere archiviate in Secrets Manager. L'archiviazione delle credenziali in Secrets Manager consente di avere il controllo e la visibilità sull'uso delle credenziali, consentendo al

contempo a Security Hub di utilizzare le credenziali per l'integrazione con l'istanza. ServiceNow Per archiviare le credenziali in Secrets Manager, è necessario utilizzare una AWS KMS chiave gestita dal cliente per proteggere i segreti. Questa AWS KMS chiave consente di proteggere i segreti mentre sono archiviati a riposo e consente inoltre di allegare una policy alla chiave che fornisce al Security Hub le autorizzazioni per accedere alla chiave che protegge il segreto.

Utilizza i seguenti passaggi per configurare Secrets Manager per ServiceNow le tue credenziali.

Fase 1: Allega una policy al tuo AWS KMS Chiave

Per configurare correttamente ServiceNow l'integrazione, devi prima concedere a Security Hub le autorizzazioni per utilizzare la AWS KMS chiave associata alle tue ServiceNow credenziali in Secrets Manager.

Per modificare il AWS KMS politica chiave per Security Hub per accedere alle tue ServiceNow credenziali

1. Apri la AWS KMS console all'indirizzo https://console.aws.amazon.com/kms.
2. Per cambiare la AWS regione, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Seleziona una AWS KMS chiave esistente o esegui i passaggi per creare una nuova chiave nella Guida per gli sviluppatori.AWS KMS
4. Nella sezione Key policy (Policy chiave), scegli Edit (Modifica).
5. Se è visualizzata la visualizzazione Passa alla politica, selezionala per visualizzare la politica chiave, quindi scegli Modifica.
6. Copia il seguente blocco di policy nella tua policy AWS KMS chiave, per concedere a Security Hub il permesso di usare la tua chiave.

```
{
    "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. Modifica la policy sostituendo i seguenti valori nell'esempio di policy:
   - *your-account-id*Sostituiscilo con l'ID AWS del tuo account.
   - Sostituiscilo *your-region* con la tua AWS regione (ad esempio,`us-east-1`).
8. Se hai aggiunto l'informativa prima dell'informativa finale, aggiungi una virgola prima di aggiungere questa dichiarazione. Assicurati che la sintassi JSON della tua policy AWS KMS chiave sia valida.
9. Selezionare Salva.
10. (Facoltativo) Copiate la chiave ARN su un blocco note per utilizzarla nei passaggi successivi.

Fase 2: Creare il segreto in Secrets Manager

Crea un segreto in Secrets Manager che memorizzerà ServiceNow le tue credenziali. Security Hub accederà a questo segreto quando interagirà con l' ServiceNow ambiente.

Segui i passaggi per creare un segreto nella Guida per l'AWS Secrets Manager utente. Dopo aver creato il segreto, copia l'ARN segreto poiché ti servirà per creare il connettore Security Hub.

Quando crei il segreto, assicurati di configurare quanto segue:

Tipo segreto

Other type of secret (Altro tipo di segreto)

Key/value coppie (formato testo semplice)

```
{
    "ClientId": "your-servicenow-client-id",
    "ClientSecret": "your-servicenow-client-secret"
    }
```

> **Note**
>
> I nomi dei campi devono essere esattamente `ClientId` e `ClientSecret` (distinzione tra maiuscole e minuscole). Security Hub richiede questi nomi esatti per recuperare le credenziali.

Chiave di crittografia

Usa la AWS KMS chiave che hai configurato nel passaggio 1

Politica delle risorse

Utilizza la policy delle risorse seguente:

```
{
    "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:*"
            }
        }
```

```
        }
    ]
    }
```

Ora che il tuo segreto è configurato, puoi creare un connettore Security Hub utilizzando l'API o la AWS console CreateConnector V2. Dovrai fornire:

- InstanceName: L'URL della tua ServiceNow istanza (ad esempio,`your-instance.service-now.com`)
- SecretArn: L'ARN del segreto creato in questa procedura

Configura un'integrazione per ServiceNow ITSM

Security Hub può creare incidenti o problemi automaticamente inServiceNow ITSM.

Per configurare un'integrazione per ServiceNow ITSM

1. Accedi al tuo AWS account con le tue credenziali e apri la console Security Hub all'indirizzohttps://console.aws.amazon.com/securityhub/v2/home? region=us-east-1.
2. Dal riquadro di navigazione, scegli Gestione, quindi scegli Integrazioni.
3. In ServiceNow ITSM, scegli Aggiungi integrazione.
4. Per i dettagli, inserisci un nome per l'integrazione e determina se inserire una descrizione opzionale per l'integrazione.
5. Per Encryptions, scegli come crittografare le tue credenziali di integrazione all'interno di Security Hub.
    - Usa chiave AWS proprietaria: con questa opzione, viene utilizzata una chiave di servizio di proprietà di Security Hub per crittografare i dati delle credenziali di integrazione all'interno di Security Hub.
    - Scegli una chiave KMS diversa (avanzata): con questa opzione scegli una chiave che hai creato e AWS KMS key che desideri utilizzare per crittografare i dati delle credenziali di integrazione all'interno di Security Hub. Per informazioni su come creare una AWS KMS chiave, consulta Create a AWS KMS key nella Developer Guide. AWS Key Management Service Se scegli di utilizzare la tua chiave, devi aggiungere dichiarazioni politiche alla chiave KMS che consentano l'accesso al Security Hub alla chiave. Consulta le politiche AWS KMS chiave per le integrazioni dei ticket di Security Hub per i dettagli sulle politiche necessarie.

> **Note**
>
> Non è possibile modificare queste impostazioni una volta completata questa configurazione. Tuttavia, se si sceglie Chiave personalizzata, è possibile modificare la politica relativa alle chiavi personalizzate in qualsiasi momento.

6. Per le credenziali, inserisci ServiceNow ITSM l'URL e l'ARN del AWS Secrets Manager tuo segreto generato nella sezione dei prerequisiti.
7. Per i tag, stabilisci se creare e aggiungere un tag opzionale alla tua integrazione.
8. Scegli Aggiungi integrazione. Dopo aver completato la configurazione, puoi visualizzare le integrazioni configurate nella scheda Integrazioni configurate.

Dopo aver configurato l'integrazione con ServiceNow, puoi testare la connessione per confermare che tutto sia configurato correttamente nel tuo ServiceNow ambiente e in Security Hub. Per ulteriori informazioni, consulta Testare le integrazioni di ticketing configurate.

Creare un ticket per un ServiceNow ITSM integrazione

Dopo aver creato un'integrazione conServiceNow ITSM, puoi creare un ticket per una ricerca.

> **Note**
>
> Un reperto sarà sempre associato a un singolo ticket durante l'intero ciclo di vita. Security Hub invia tutti gli aggiornamenti successivi a un risultato dello stesso ticket dopo la creazione iniziale. Se un connettore associato a una regola di automazione viene modificato, il connettore aggiornato viene utilizzato solo per i risultati nuovi e in arrivo che soddisfano i criteri della regola.

Per creare un ticket per una scoperta

1. Accedi al tuo AWS account con le tue credenziali e apri la console Security Hub all'indirizzohttps://console.aws.amazon.com/securityhub/v2/home? region=us-east-1.
2. Dal pannello di navigazione, in Inventario, scegli Risultati.
3. Scegli un risultato. Nella ricerca, scegli Crea biglietto.
4. Per l'integrazione, apri il menu a discesa e scegli un'integrazione.

5. Scegli Crea.

Visualizzazione di un ticket per un ServiceNow ARTICOLO M integrazione

Dopo aver creato un ticket per una ricerca, puoi aprirlo sulla tua ServiceNow ITSM istanza.

Per visualizzare un risultato sul tuo ServiceNow ARTICOLO M istanza

1. Accedi al tuo AWS account con le tue credenziali e apri la console Security Hub all'indirizzohttps://console.aws.amazon.com/securityhub/v2/home? region=us-east-1.
2. Dal pannello di navigazione, in Inventario, scegli Risultati.
3. Scegli il risultato in cui hai creato il ticket.
4. Nella ricerca, scegli l'ID del ticket per visualizzare il ticket sulla tua ServiceNow ITSM istanza o Visualizza JSON.

Politiche chiave KMS per le integrazioni di ticketing di Security Hub

Quando si utilizzano chiavi KMS gestite dal cliente con integrazioni di ticketing Security Hub, è necessario aggiungere politiche aggiuntive alla chiave KMS per consentire a Security Hub di interagire con la chiave. Inoltre, è necessario aggiungere politiche che consentano al principale che aggiunge la chiave alle autorizzazioni del connettore Security Hub di accedere alla chiave.

Politica sulle autorizzazioni di Security Hub

La seguente politica delinea le autorizzazioni necessarie a Security Hub per poter accedere e utilizzare la chiave KMS associata a Jira e ai connettori. ServiceNow Questa policy deve essere aggiunta a ogni chiave KMS associata a un connettore Security Hub.

La policy contiene le seguenti autorizzazioni:

- Consente a Security Hub di proteggere, accedere temporaneamente o aggiornare i token utilizzati per comunicare con le integrazioni di ticketing, utilizzando la chiave. Le autorizzazioni sono limitate alle operazioni relative a specifici connettori Security Hub tramite il blocco di condizioni che verifica l'ARN di origine e il contesto di crittografia.
- Consente a Security Hub di leggere i metadati sulla chiave KMS consentendone l'operazione. `DescribeKey` Questa autorizzazione è necessaria affinché Security Hub verifichi lo stato e la configurazione della chiave. L'accesso è limitato a connettori Security Hub specifici tramite la condizione ARN di origine.

```
{
    "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/*"
        }
    }
}
```

Modifica la policy sostituendo i seguenti valori nell'esempio di policy:

- Sostituisci *CloudProviderName* con JIRA_CLOUD o SERVICENOW
- Sostituisci *AccountId* con l'ID dell'account in cui stai creando il connettore Security Hub.
- Sostituiscilo *Region* con la tua AWS regione (ad esempio,us-east-1).

Accesso principale IAM per le operazioni di Security Hub

Qualsiasi principale che assegna chiavi KMS gestite dal cliente a un connettore Security Hub deve disporre delle autorizzazioni per eseguire le operazioni chiave (descrizione, generazione, decrittografia, ricrittografia ed elenco degli alias) per la chiave da aggiungere al connettore. Questo CreateTicket vale per le API V2 e V2. CreateConnector La seguente dichiarazione politica deve essere inclusa come parte della politica per tutti i principali che interagiscono con queste API.

```
{
    "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"
            ]
        }
    }
}
```

Modifica la policy sostituendo i seguenti valori nell'esempio di policy:

- Sostituisci *RoleName* con il nome del ruolo IAM che effettua chiamate a Security Hub.
- Sostituisci *CloudProviderName* con `JIRA_CLOUD` o `SERVICENOW`.
- Sostituisci *AccountId* con l'ID dell'account in cui stai creando il connettore Security Hub.
- Sostituiscilo *Region* con la tua AWS regione (ad esempio,`us-east-1`).

Test delle integrazioni di ticketing configurate

Per Jira e ServiceNow le integrazioni configurate, puoi testare la connessione per assicurarti che tutta la configurazione in Security Hub e nel tuo ambiente Jira o sia completa. ServiceNow

La funzione test ticket crea un ticket con il titolo di. `TESTING Test CreateTicketV2 Finding` Il ticket di test è compilato con dati di esempio come l'ID dell'account e la regione dell'account in cui viene eseguito il test, i dettagli delle risorse di esempio e il codice JSON di AWS ricerca di esempio.

Test delle integrazioni tramite la console

Usa i seguenti passaggi per testare la tua integrazione:

1. Nel pannello di navigazione di Security Hub, scegli Integrazioni.
2. Nella scheda Integrazioni configurate, scegli l'integrazione che desideri testare.
3. Nella pagina di panoramica dell'integrazione, scegli Crea ticket di test.

4. Security Hub mostra un messaggio di esito positivo e un link al ticket di test se il test ha esito positivo. Se il test non ha esito positivo, Security Hub visualizza un errore. In base al messaggio di errore, risolvi i problemi di configurazione in Security Hub o nel tuo Jira ServiceNow ambiente operativo.

> **Note**
>
> La funzionalità del ticket di test ha lo scopo di aiutare a verificare la funzionalità end-to-end per la configurazione di una nuova connessione o quando si apportano modifiche a una connessione esistente. Questa funzionalità crea un nuovo ticket nel tuo Jira ServiceNow ambiente ogni volta che viene utilizzata e non è destinata alla verifica regolare della connessione.

Test con AWS CLI

Per testare l'integrazione utilizzando il AWS CLI, usa il `create-ticket-v2` comando con il `--mode DRYRUN` parametro:

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region <your-region> \
  --connector-id <your-connector-id> \
  --finding-metadata-uid "TEST_FINDING"
```

Esempio

L'esempio seguente mostra come testare un'integrazione:

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region us-east-1 \
  --connector-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
  --finding-metadata-uid "TEST_FINDING"
```

Risposta riuscita

Una risposta corretta restituisce quanto segue:

```
{
    "TicketId": "a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6",
    "TicketSrcUrl": "https://your-instance.service-now.com/nav_to.do?
uri=x_aws_se_0_finding.do?sys_id=a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6"
}
```

`TicketSrcUrl`Nella risposta fornisce un link diretto per visualizzare il ticket di test in Jira o nell' ServiceNow ambiente.

Se il test fallisce, viene visualizzato un messaggio di errore che indica il problema di configurazione da risolvere.

Risoluzione degli errori di integrazione con Jira cloud

Durante il test dell'integrazione Jira Cloud da Security Hub, potrebbero essere restituiti i seguenti messaggi di errore. Questi messaggi di errore possono fornire informazioni su dove potrebbe essere il problema di configurazione con il connettore e su come risolverlo.

Messaggi di errore relativi all'integrazione con Jira Cloud

Errore	Messaggio di errore	Probabile causa e risoluzione
ConflictException	Impossibile trovare il progetto jira	Causa probabile: il progetto sul connettore non è corretto o credentials/permissions un problema ci impedisce di accedere al progetto. Probabile soluzione: aggiungi il progetto corretto al connettore o esegui nuovamente l'autenticazione su Jira con le credenziali corrette.
ConflictException	Tipo di problema di Security Hub non trovato	Causa probabile: il problema o il tipo di problema relativo all'installazione dell'app non è associato al progetto.

Errore	Messaggio di errore	Probabile causa e risoluzione
		Probabile soluzione: esegui il passaggio preliminare per installar e l'app Jira nel tuo ambiente Jira e associa l'app al progetto.

App MCP (anteprima)

Security Hub offre un'esperienza agentica con un'app Model Context Protocol (MCP). Con questa app, il tuo agente AI può esaminare i risultati dell'esposizione. Può anche diagnosticare un connettore di Azure esistente o valutare i prerequisiti del connettore di Azure prima della creazione.

Ogni chiamata allo strumento di ricerca restituisce un riepilogo testuale su cui l'agente deve ragionare. Se disponibile, restituisce anche una visualizzazione interattiva da verificare nella stessa conversazione. Connector Diagnostics restituisce un testo strutturato che separa i risultati confermati dai controlli che non è stato possibile verificare.

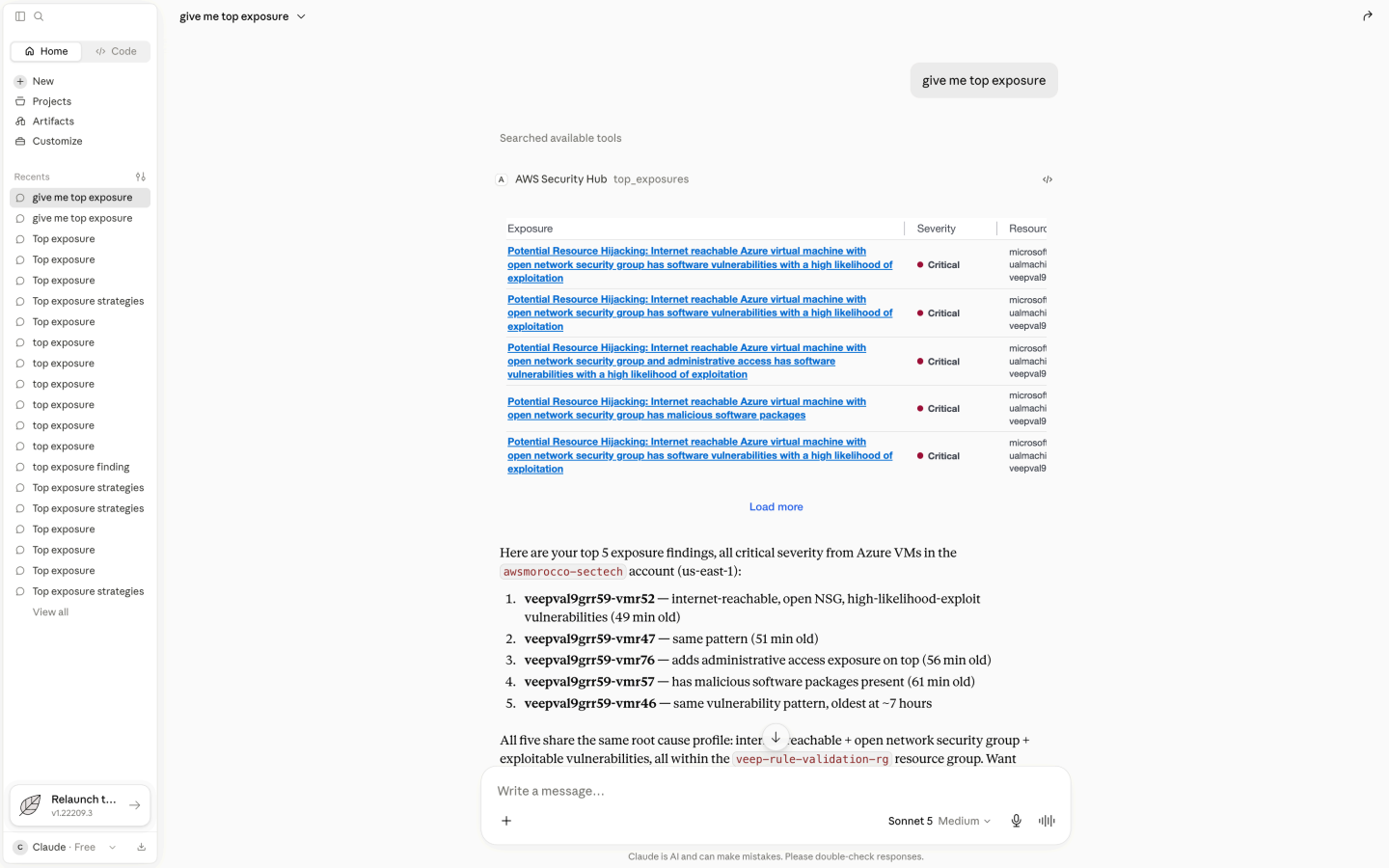
L'app MCP è un server MCP locale che viene eseguito sul computer e chiama direttamente le API Security Hub utilizzando le credenziali esistenti. AWS Connector Diagnostics può anche eseguire query CLI di Azure limitate e di sola lettura utilizzando la sessione della riga di comando di Azure esistente. Ogni strumento è di sola lettura e non modifica lo stato di sicurezza o le risorse dei connettori. L'app MCP è disponibile in tutte le regioni AWS commerciali in cui è disponibile Security Hub.

> **Important**
>
> L'app Security Hub MCP è disponibile in anteprima pubblica.

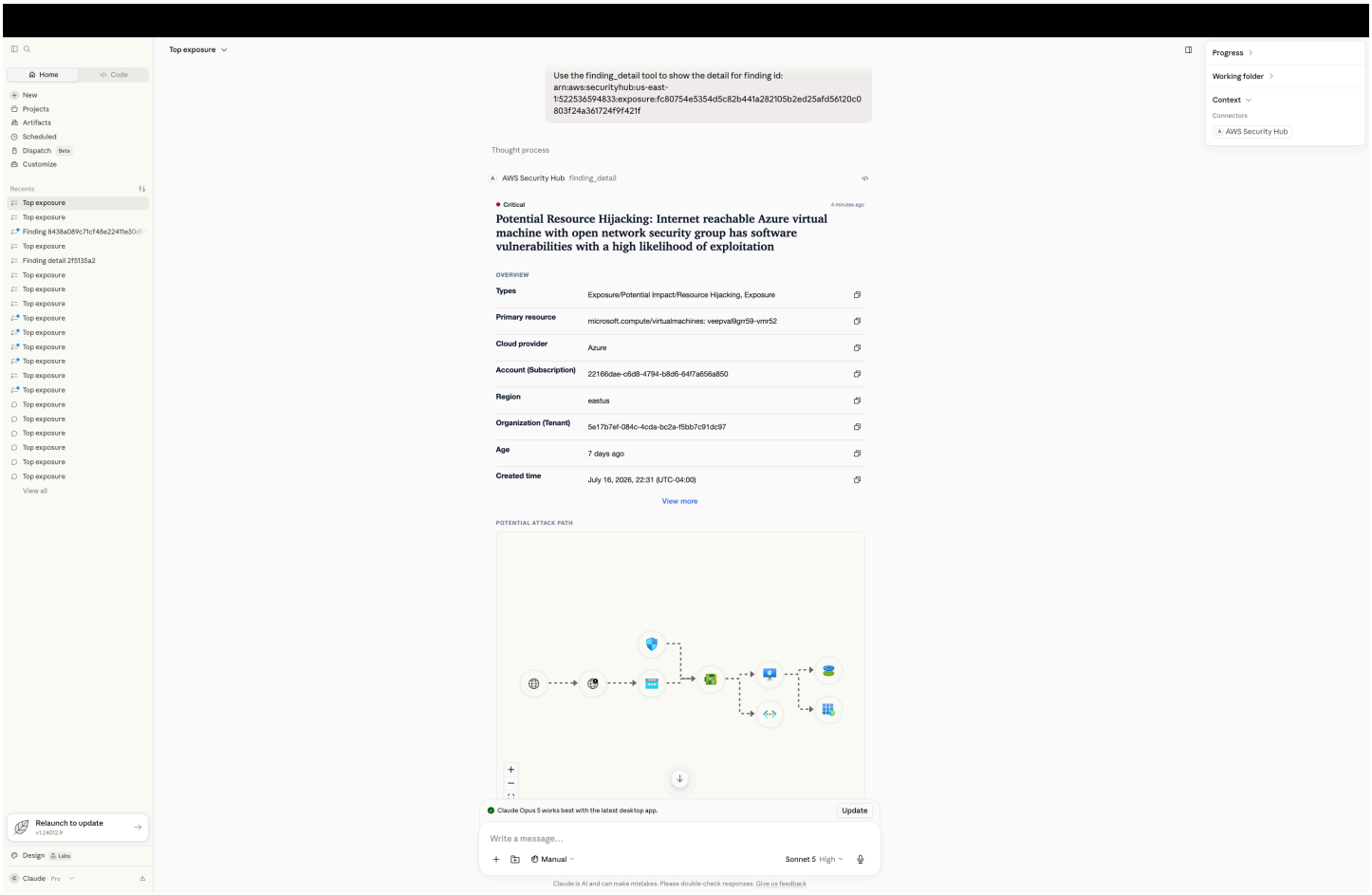
Esempi di app MCP

Gli esempi seguenti mostrano come l'app MCP esegue il rendering delle visualizzazioni interattive all'interno di Claude Desktop mentre analizzi le esposizioni.

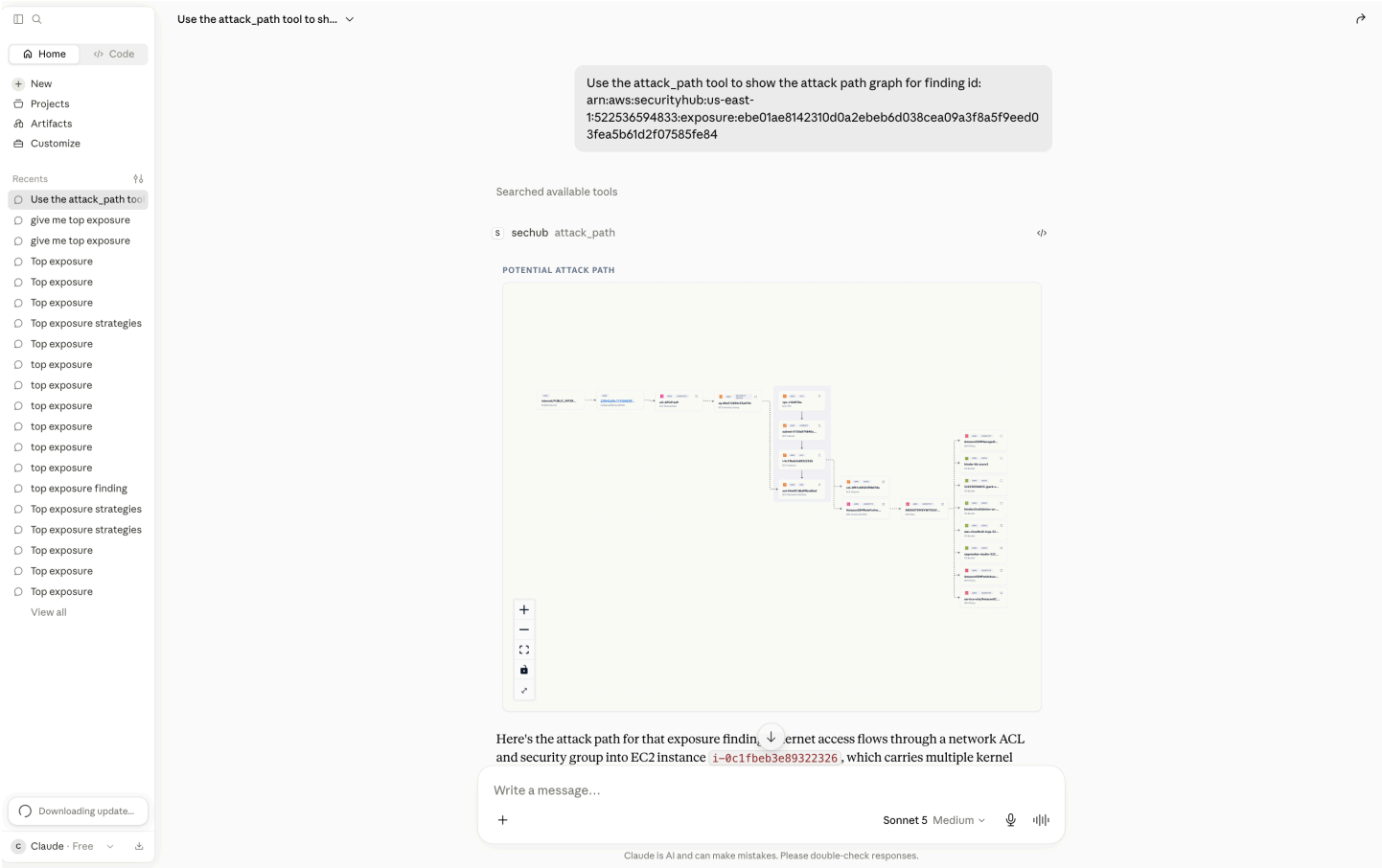
Esposizioni principali: elenca i risultati più critici relativi all'esposizione, in una tabella interattiva. L'immagine seguente mostra la tabella delle esposizioni principali.



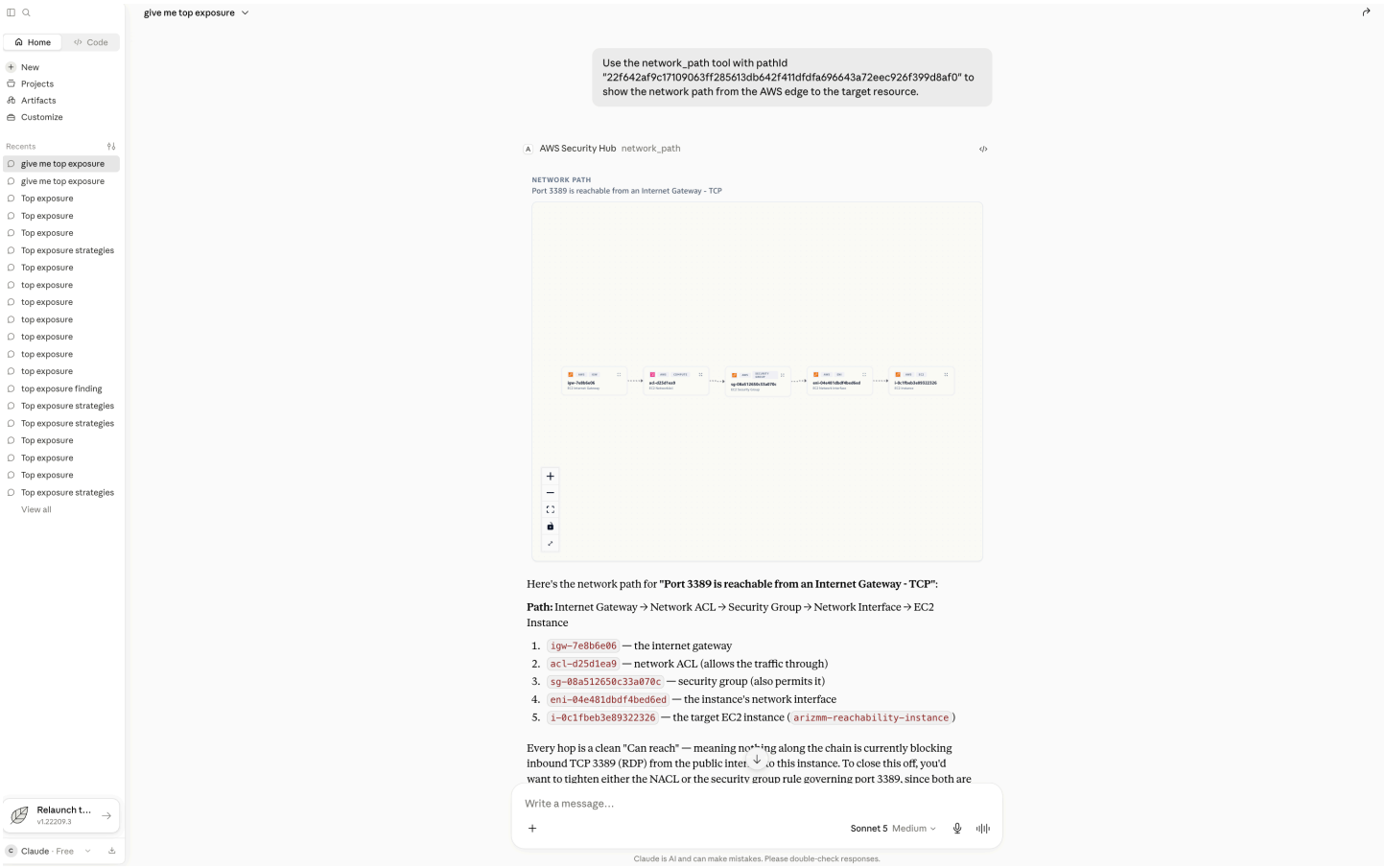
Dettagli analitici: esamina la panoramica di un singolo risultato sull'esposizione insieme al riepilogo delle caratteristiche correlate, al percorso di attacco e alle linee guida per la correzione. L'immagine seguente mostra la visualizzazione dettagliata dei risultati.



Percorso di attacco: visualizza in che modo un'esposizione è raggiungibile in un grafico interattivo. I nodi rappresentano risorse, identità e servizi. I bordi rappresentano le relazioni tra di essi. L'immagine seguente mostra il grafico del percorso di attacco.



Percorso di rete: esplora i passaggi di rete ordinati dall' AWS edge alla risorsa di destinazione (ad esempio, da Internet Gateway a NACL a Security Group a ENI to Instance). L'immagine seguente mostra il percorso di rete.



Diagnosi del connettore: chiedi perché un connettore di Azure esistente è danneggiato o non funziona. L'agente identifica i problemi confermati, distingue i controlli che non è stato possibile verificare e consiglia la minima riparazione senza modificare l'ambiente.

Disponibilità del connettore: verifica i prerequisiti di Azure prima di creare un connettore. L'agente segnala quali prerequisiti sono stati superati, non riusciti o non hanno potuto essere verificati.

Concetti chiave

Rilevamento dell'esposizione: un risultato che mette in correlazione più segnali, come vulnerabilità, configurazioni errate, raggiungibilità della rete e dati sensibili, in un'unica visualizzazione di una risorsa esposta al rischio.

Connector Diagnostics: tre strumenti di sola lettura per i connettori di Azure. Gli strumenti diagnosticano un connettore esistente, valutano una configurazione proposta e recuperano estratti esatti dallo script di configurazione di Azure supportato. ??? L'agente seleziona gli strumenti e ne traduce i risultati strutturati in una spiegazione.

Server MCP locale: un programma che viene eseguito sul computer e funge da ponte bidirezionale sicuro tra Claude Desktop e Security Hub. Il server contiene gli strumenti utilizzati dal tuo agente AI, inclusi gli strumenti per il rendering dell'interfaccia utente all'interno di Claude Desktop. Utilizza la catena di AWS credenziali della macchina e non possiede credenziali proprie.

App MCP: un'applicazione interattiva che esegue il rendering all'interno di Claude Desktop. Ogni visualizzazione dell'app MCP esegue un singolo lavoro, ad esempio mostrare la tabella delle esposizioni principali o un grafico del percorso di attacco.

Doppia risposta: una singola chiamata allo strumento di ricerca restituisce due risultati: un riepilogo testuale compatto su cui l'agente ragiona e una visualizzazione interattiva visualizzata nella stessa conversazione per essere esaminata.

Prerequisiti

- Un AWS account con Security Hub abilitato. I risultati dell'esposizione sono richiesti solo per i risultati e gli strumenti di esposizione.
- Claude Desktop installato. Per il programma di installazione, consultate il download di Claude Desktop sul sito Web di Claude.
- AWS credenziali configurate nella catena di credenziali SDK standard AWS .
- Per Azure-side Connector Diagnostics, installa l'interfaccia della riga di comando di Azure. Effettua l'autenticazione nel tenant del connettore eseguendo `az login --tenant`*`tenant-id`*, *`tenant-id`* dov'è l'ID del tenant di Azure che contiene il connettore. L'app MCP utilizza la sessione CLI locale di Azure risultante. Non aggiungere credenziali di Azure alla configurazione MCP.

> **Note**
>
> È possibile eseguire Connector Diagnostics senza una sessione dell'interfaccia della riga di comando di Azure autenticata. Il risultato include la valutazione disponibile e AWS Azure-dependent contrassegna i controlli come non verificati. Non considera mai integre le prove di Azure non disponibili.

Configurazione del server MCP

L'app MCP viene installata in Claude Desktop da un file bundle. Prima dell'installazione, verificate che l'`aws sts get-caller-identity`operazione abbia esito positivo e che `aws configure`

`get region` restituisca una regione nel terminale, in modo che il server possa leggere le vostre credenziali e la regione. AWS

1. Scarica il pacchetto Security Hub MCP App.
2. Apri il file scaricato `.mcpb`. Claude Desktop avvia un flusso di configurazione. Segui le istruzioni per installare il server.
3. Per verificare la connessione, inserisci una domanda in Claude Desktop, ad esempio «Quali sono le mie principali vulnerabilità di sicurezza?» oppure «Il mio connettore Azure in us-west-2 è danneggiato. Riesci a determinare cosa non va?» Se ricevi un errore, consulta le indicazioni contenute nel messaggio di errore e conferma le tue credenziali e la regione.

Utilizzo di Connector Diagnostics

Descrivi il problema del connettore o la configurazione proposta in linguaggio naturale. L'agente seleziona lo strumento di sola lettura appropriato, ne interpreta il risultato strutturato e indica quali controlli sono stati confermati e quali no.

Diagnostica un connettore esistente

1. Identifica il connettore in base al relativo ID o al nome esatto. Fornisci anche l' AWS account e la regione che contengono il connettore se l'agente non è in grado di determinarli dalla tua richiesta.
2. Fai una domanda del tipo «Il mio connettore di Azure in us-west-2 è danneggiato. Puoi determinare cosa c'è che non va e dirmi cosa correggere prima?»
3. Esamina i risultati confermati separatamente dai controlli che non sono stati verificati. Quando l'autenticazione di Azure non è disponibile, l'agente limita le sue conclusioni alle prove AWS secondarie.

Valuta un connettore proposto

1. Fornisci l' AWS account, la AWS regione e l'ID del tenant di Azure. Fornisci inoltre da 1 a 10 ID di sottoscrizione di Azure che verranno coperti dal connettore proposto. Indica all'agente quali prerequisiti del servizio valutare: Cloud Security Posture Management (CSPM), scansione della macchina virtuale Inspector o rilevamento delle minacce. Queste selezioni comprendono i controlli di idoneità. Non sono impostazioni per la creazione di connettori.

2. Fai una domanda come «Prima di creare il mio connettore di Azure, controlla se i prerequisiti sono pronti per queste sottoscrizioni».
3. Esamina i controlli superati, non riusciti e non verificati. Un risultato di idoneità corretto indica che i prerequisiti verificati sono stati superati. Ciò non significa che un connettore esista, sia in esecuzione o sia stato ripristinato.

Recupera le istruzioni di configurazione

Se un risultato si riferisce a una fase di onboarding, chiedi all'agente di mostrarla. Ad esempio, chiedi «Mostrami il passaggio 6 dello script di configurazione del connettore di Azure supportato». Per lo script completo, vedi Configurazione di Microsoft Azure per l'integrazione con Security Hub. Lo strumento restituisce un estratto esatto ma non lo esegue. Esegui lo script supportato completo perché i suoi passaggi condividono le funzioni di configurazione e di supporto.

> **Note**
>
> Connector Diagnostics non ripara o modifica mai le risorse. La correzione è una guida per un'azione separata che puoi controllare. La diagnosi riporta il ripristino solo quando nuove prove in fase di esecuzione lo dimostrano.

Strumenti disponibili

`top_exposures`— Elenca i risultati più urgenti relativi all'esposizione in una tabella interattiva. Chiamate innanzitutto questo strumento perché gli strumenti di per-finding richiedono un ID di ricerca incluso in questo elenco.

`finding_detail`— Restituisce la panoramica di un risultato, incluso il riepilogo delle caratteristiche dei risultati correlati.

`finding_overview`— Restituisce un riepilogo testuale di un risultato mediante la ricerca dell'ID.

`correlated_finding_detail`— Elenca i risultati correlati a un'esposizione per un singolo tratto, ad esempio Vulnerabilità, Errata configurazione o Raggiungibilità.

`attack_path`— Crea il grafico del percorso di attacco per un risultato.

`network_path`— Espande il percorso di rete di un reperto in salti ordinati dall' AWS edge alla risorsa bersaglio.

`recommendation`— Restituisce le linee guida per la risoluzione di un risultato, inclusi i collegamenti alla documentazione.

`resource_detail`— Restituisce la configurazione di una AWS risorsa tramite ID breve (ad esempio`i-1234`) o ARN.

`diagnose_connector`— Diagnostica un connettore di Azure esistente utilizzando lo stato del Security Hub e le prove limitate dell'interfaccia della riga di comando di Azure, se disponibili. Restituisce i risultati confermati, l'ambito interessato, le linee guida per la correzione e l'aggiornamento dei dati. Elenca inoltre tutti i controlli che non è stato possibile verificare.

`assess_connector_readiness`— Valuta il AWS lato e i Azure-side prerequisiti di un connettore di Azure proposto prima della creazione. Non crea un connettore.

`get_connector_setup_instructions`— Restituisce estratti esatti dallo script di onboarding di Azure pacchettizzato e supportato. Non esegue lo script.

Monitoraggio dell'utilizzo e dei costi in Security Hub

La pagina Utilizzo ti aiuta a comprendere e a gestire i costi di gestione di Security Hub in tutta l'organizzazione. Da questa pagina, puoi visualizzare i costi correnti, vedere i costi mensili previsti, esplorare l'utilizzo per funzionalità o per account e trovare strategie per ottimizzare la spesa.

Chi può accedere alla pagina Utilizzo

La pagina Utilizzo è disponibile da qualsiasi account con Security Hub abilitato. Per accedervi, apri la console Security Hub e scegli Utilizzo in Impostazioni nel pannello di navigazione.

> **Important**
>
> Se il tuo account è un account membro di un' AWS organizzazione e non è stato designato un amministratore delegato di Security Hub, i dati di utilizzo non sono disponibili. Per visualizzare i dati di utilizzo, l'account di gestione dell'organizzazione deve designare un amministratore delegato. Per ulteriori informazioni, consulta the section called "Designazione di un amministratore delegato".

L'esperienza varia a seconda del tipo di account:

- Amministratore delegato o account di gestione: viene visualizzata la pagina di utilizzo completa con un riepilogo dei costi dell'organizzazione, l'utilizzo per capacità, l'utilizzo per account e le strategie di ottimizzazione dei costi.
- Account membro o account autonomo: viene visualizzato un riepilogo dei costi dell'account con utilizzo per funzionalità solo per il tuo account. La scheda Per account non è disponibile perché stai visualizzando un singolo account.

Riepilogo dei costi dell'organizzazione e dell'account

> **Note**
>
> La sezione di riepilogo dei costi dell'organizzazione è visibile solo dall'account amministratore delegato o dall'account di gestione. Gli account membri e gli account autonomi visualizzano invece un riepilogo dei costi dell'account.

Quando si apre la pagina Utilizzo da un amministratore delegato o da un account di gestione, la sezione Riepilogo dei costi dell'organizzazione mostra una panoramica di alto livello dei costi del Security Hub dell'organizzazione per il ciclo di fatturazione corrente. Questa sezione include quanto segue:

- Ultimo aggiornamento dei dati: la data in cui Security Hub ha aggiornato l'ultima volta i dati di utilizzo per l'organizzazione. Security Hub aggiorna questi dati periodicamente. Se i dati risalgono a più di 24 ore quando visiti la pagina Utilizzo, Security Hub attiva automaticamente un aggiornamento. L'aggiornamento viene completato entro poche ore, a seconda delle dimensioni dell'organizzazione. Durante l'aggiornamento dei dati, viene visualizzato un avviso con un messaggio che indica che i dati saranno disponibili a breve.
- Costi correnti: l'importo totale sostenuto dall'organizzazione per l'utilizzo di Security Hub dall'inizio del ciclo di fatturazione corrente fino alla data dell'ultimo aggiornamento dei dati.
- Costi mensili previsti (30 giorni): costo mensile stimato basato sugli ultimi 7 giorni di utilizzo, estrapolato a un ciclo di fatturazione completo di 30 giorni. Questa proiezione include l'utilizzo della versione di prova a pagamento e gratuita per fornire una stima realistica dei costi mensili. I costi previsti non tengono conto degli eventuali sconti (EDP) con cui avete negoziato. AWS Se i costi previsti sembrano inferiori ai costi attuali, significa che l'utilizzo è diminuito e, in base agli ultimi 7 giorni di utilizzo, la fattura di 30 giorni sarà inferiore alla fattura del ciclo di fatturazione corrente.

Visualizzazione delle capacità

La visualizzazione delle capacità mostra i costi e l'utilizzo nell'intera organizzazione, organizzati per funzionalità di sicurezza. Le funzionalità sono organizzate in tre gruppi espandibili. Puoi espandere o comprimere ciascun gruppo per visualizzare i singoli tipi di utilizzo al suo interno. Ogni tipo di utilizzo è associato direttamente a un tipo di utilizzo corrispondente in AWS Cost Explorer.

Piano Security Hub essentials: monitora le istanze EC2, le immagini dei container ECR, le funzioni Lambda, gli utenti IAM e i ruoli IAM. Copre l'analisi dei rischi e dell'esposizione, la gestione delle vulnerabilità (con tecnologia Amazon Inspector), la gestione del livello di sicurezza (con tecnologia Security Hub CSPM) e la risposta alla sicurezza. Tutte queste funzionalità sono incluse nel piano Essentials a un prezzo unico per risorsa: non è necessario abilitare o pagare separatamente Amazon Inspector o AWS Security Hub CSPM e non è previsto un doppio addebito per l'utilizzo del servizio sottostante.

Analisi delle minacce: include eventi di CloudTrail gestione ed eventi relativi ai dati, attività di rete e altri registri. Queste funzionalità coprono il rilevamento delle minacce con tecnologia Amazon GuardDuty.

Funzionalità aggiuntive: include la scansione del codice delle funzioni Lambda. Si tratta di un miglioramento opzionale fornito da Amazon Inspector per l'analisi del codice applicativo della funzione Lambda alla ricerca di vulnerabilità di sicurezza.

Per ulteriori informazioni sui prezzi di ciascuna funzionalità, consulta i prezzi di Security Hub. https://aws.amazon.com/security-hub/pricing/

La tabella in questa visualizzazione include le seguenti colonne per ogni tipo di utilizzo:

- Utilizzo corrente: il volume di utilizzo totale per questo tipo di utilizzo dall'inizio del ciclo di fatturazione fino alla data dell'ultimo aggiornamento dei dati, in tutti gli account e in tutte le aree geografiche.
- Utilizzo gratuito: il volume di utilizzo totale per questo tipo di utilizzo da parte degli account attualmente in prova gratuita. I valori di utilizzo gratuito vengono visualizzati in verde.
- Costi correnti: il costo totale per questo tipo di utilizzo dall'inizio del ciclo di fatturazione fino alla data dell'ultimo aggiornamento dei dati, per tutti gli account e tutte le aree geografiche.
- Valore della versione di prova gratuita: il costo che avresti sostenuto per questo tipo di utilizzo se gli account attualmente in prova gratuita non lo fossero. Questo ti aiuta a comprendere il valore della prova gratuita.

- Costi mensili previsti (30 giorni): il costo mensile stimato per questo tipo di utilizzo, estrapolato dagli ultimi 7 giorni di utilizzo per tutti gli account e tutte le aree geografiche. Ciò include l'utilizzo della versione di prova a pagamento e gratuita per fornire una stima del costo mensile.

Visualizzazione dell'account

> **Note**
>
> La visualizzazione dell'account è disponibile solo dall'account amministratore delegato o dall'account di gestione.

Scegli la visualizzazione dell'account per visualizzare i costi organizzati dagli account dei singoli membri in tutte le regioni. Questa visualizzazione consente di identificare gli account che generano i costi maggiori.

La tabella elenca ogni account con le seguenti colonne:

- Account: l' Account AWS ID, visualizzato come link cliccabile. La scelta di un account apre un pannello dettagliato di suddivisione.
- Costi correnti: il costo totale di questo account dall'inizio del ciclo di fatturazione fino alla data dell'ultimo aggiornamento dei dati, in tutte le regioni.
- Valore della versione di prova gratuita: il costo che questo account avrebbe sostenuto se non fosse stato incluso nella prova gratuita.
- Costi mensili previsti (30 giorni): costo mensile stimato per questo account, estrapolato dagli ultimi 7 giorni di utilizzo in tutte le regioni a un ciclo di fatturazione completo di 30 giorni. La proiezione include l'utilizzo della versione di prova gratuita e a pagamento per fornire una stima rappresentativa dei costi mensili. I costi previsti non tengono conto degli sconti negoziati con AWS (EDP).

  Se Security Hub è stato abilitato su questo account negli ultimi 7 giorni, la proiezione si basa sul numero di giorni trascorsi dall'attivazione. Dopo 7 giorni, la proiezione utilizza tutti gli ultimi 7 giorni di utilizzo. La pagina Utilizzo attualmente non rileva quando Security Hub è stato disabilitato su un account. Se Security Hub è stato recentemente disabilitato su uno o più account, tali account continuano a comparire nella proiezione fino alla scadenza del loro utilizzo. Attendi 7 giorni dopo aver apportato queste modifiche affinché la proiezione rifletta lo stato aggiornato della tua organizzazione.

Visualizzazione dei dettagli dell'account

Quando scegli un account dall'elenco, si apre un pannello dei dettagli sul lato destro della pagina. Questo pannello mostra la stessa suddivisione dei livelli di funzionalità della vista Capacità, ma filtrata in base a quell'account specifico. Puoi visualizzare l'utilizzo corrente, l'utilizzo gratuito, i costi correnti, il valore della prova gratuita e i costi mensili previsti per ogni tipo di utilizzo all'interno di quell'account, in tutte le aree geografiche.

Strategie di ottimizzazione dei costi

Scegli le strategie di ottimizzazione dei costi nella pagina Utilizzo per accedere a una pagina dedicata con modi pratici per gestire i costi mantenendo la copertura di sicurezza.

Ogni strategia è presentata come un'opzione indipendente che puoi valutare e applicare in base alle esigenze della tua organizzazione. Le opzioni senza compromessi in termini di sicurezza sono elencate per prime. Dopo aver applicato una strategia, le modifiche richiedono in genere dalle 24 alle 48 ore per essere riportate nella fatturazione.

Risorse correlate

- Prezzi di Security Hub
- AWS Guida utente di Cost Explorer

Disattivazione di Security Hub

Disattivazione di Security Hub per un singolo account

Se il tuo account non fa parte di un'organizzazione, puoi disattivare Security Hub nella console Security Hub in qualsiasi momento o utilizzare l'DisableSecurityHubV2 API. Quando disabiliti Security Hub, smette di acquisire i risultati dai motori di rilevamento e perdi anche l'accesso ai risultati, alle integrazioni e alle configurazioni esistenti.

Quando disabiliti Security Hub per il tuo account in tutte le regioni, Security Hub elimina anche l'IAM Access Analyzer collegato al servizio che è stato creato quando hai abilitato il servizio. Se l'eliminazione automatica non riesce, puoi eliminare l'analizzatore richiamando l'operazione API IAM Access Analyzer. `DeleteServiceLinkedAnalyzer` Questa operazione ha esito positivo solo dopo che Security Hub è stato completamente disabilitato per il tuo account. Se disabiliti Security Hub in

una singola regione ma rimani abilitato in altre regioni, l'analizzatore degli accessi inutilizzati continua a funzionare e i risultati continuano a essere replicati nelle restanti regioni abilitate.

Come disabilitare Centrale di sicurezza

1. Accedi al tuo AWS account con le tue credenziali e apri la console di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
2. Dal pannello di navigazione, scegli Generale.
3. In Security Hub, scegli Disabilita. Nella finestra pop-up**`Disable`**, inserisci e scegli Disabilita.

Disattivazione di Security Hub in un'organizzazione

Se sei l'amministratore delegato di un' AWS organizzazione, hai due opzioni per disabilitare Security Hub tra gli account dei membri.

Opzione 1: disattivazione di Security Hub con motori di rilevamento

Puoi sfruttare la distribuzione e la policy di Security Hub (funzionalità essenziali e aggiuntive) dal catalogo delle politiche nel tuo account di amministratore delegato per disabilitare Security Hub insieme ad Amazon Inspector per unità organizzative, account o regioni specifici.

Per disattivare Security Hub e Amazon Inspector tra gli account membri utilizzando una policy

1. Accedi utilizzando il tuo AWS account con le credenziali di amministratore delegato. Apri la console Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
2. Dal pannello di navigazione, scegli Gestione, quindi scegli Configurazioni.
3. Scegli Security Hub (funzionalità essenziali e aggiuntive) dal catalogo di configurazione.
4. Nella pagina Configura Security Hub nella sezione Dettagli, inserisci un nome e una descrizione per la policy (ad esempio, «Politica di disattivazione di Security Hub»).
5. Nella sezione Selezione dell'account, seleziona una delle seguenti opzioni. Scegli Tutte le unità organizzative e gli account se desideri applicare la disattivazione a tutte le unità organizzative e gli account. Scegli Unità organizzative e account specifici se desideri applicare la disattivazione a unità organizzative e account specifici. Se scegli questa opzione, utilizza la barra di ricerca o l'albero della struttura organizzativa per specificare le unità organizzative e gli account di destinazione.

6. Nella sezione Regioni, scegli Disabilita tutte le regioni per disabilitare Security Hub in tutte le regioni. Facoltativamente, scegli se disabilitare automaticamente le nuove regioni. Scegli Specifica regioni per scegliere quali regioni specifiche vuoi disattivare.
7. (Facoltativo) Per le impostazioni avanzate, consulta le indicazioni di AWS Organizations.
8. (Facoltativo) Per i tag Resource, aggiungete i tag come coppie chiave-valore per identificare facilmente la configurazione.
9. Scegli Next (Successivo).
10. Rivedi le modifiche, quindi scegli Applica. Gli account di destinazione sono configurati in base alla policy. Lo stato di configurazione della politica viene visualizzato nella parte superiore della pagina Politiche.

Disattivazione di Amazon GuardDuty e AWS Security Hub CSPM

Per quanto riguarda GuardDuty le funzionalità CSPM di Security Hub, è necessario disabilitare manualmente le funzionalità dai rispettivi account di amministratore delegato. GuardDuty e Security Hub CSPM utilizzano le distribuzioni (azioni una tantum) anziché le policy, pertanto la disattivazione deve essere eseguita manualmente dalle rispettive console.

Opzione 2: disabilitazione solo di Security Hub

Se disponi di una policy Security Hub esistente e desideri disabilitare solo Security Hub, senza influire su Amazon Inspector o Security Hub CSPM, segui questi passaggi. GuardDuty

Per disabilitare Security Hub solo tra gli account membri

1. Accedi utilizzando il tuo AWS account con le credenziali di amministratore delegato. Apri la console Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/v2/home
2. Dal pannello di navigazione, scegli Gestione, quindi scegli Configurazioni.
3. Scegli una delle tue politiche di Security Hub tra le politiche configurate.
4. Scegli Modifica politica e nella sezione di selezione dell'account, seleziona una delle seguenti opzioni. Scegli Tutte le unità organizzative e gli account se desideri applicare la disattivazione a tutte le unità organizzative e gli account. Scegli Unità organizzative e account specifici se desideri applicare la disattivazione a unità organizzative e account specifici. Se scegli questa opzione, utilizza la barra di ricerca o l'albero della struttura organizzativa per specificare le unità organizzative e gli account di destinazione.

5. Nella sezione Regioni, scegli Disabilita tutte le regioni per disabilitare Security Hub in tutte le regioni. Facoltativamente, scegli se disabilitare automaticamente le nuove regioni. Scegli Specifica regioni per scegliere quali regioni specifiche vuoi disattivare.
6. (Facoltativo) Per le impostazioni avanzate, consulta le linee guida fornite dalle AWS organizzazioni.
7. (Facoltativo) Per i tag Resource, aggiungete i tag come coppie chiave-valore per identificare facilmente la configurazione.
8. Scegli Next (Successivo).
9. Rivedi le modifiche, quindi scegli Applica. Gli account di destinazione sono configurati in base alla policy. Lo stato di configurazione della policy viene visualizzato nella parte superiore della pagina Configurazioni.

Impatto su altri servizi di sicurezza

La disabilitazione di Security Hub tramite una policy di Security Hub non ha alcun impatto sulle configurazioni di Security Hub GuardDuty, CSPM e Amazon Inspector.

Se devi disabilitare Amazon Inspector solo tra gli account membri, puoi utilizzare la politica di gestione delle vulnerabilità dal catalogo di configurazione di Security Hub. Accedi alla pagina di configurazione di Security Hub, scegli Gestione delle vulnerabilità da Amazon Inspector e crea una policy di disabilitazione seguendo passaggi simili alla procedura di disabilitazione di Security Hub riportata sopra.

Sicurezza in AWSSecurity Hub

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWSti fornisce anche servizi che puoi utilizzare in modo sicuro. Third-partyi revisori testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei programmi di AWSconformità. Per ulteriori informazioni sui programmi di conformità che si applicano a Security Hub, vedere AWSServizi nell'ambito del programma di conformità.

- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Security Hub. I seguenti argomenti mostrano come configurare Security Hub per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le risorse del Security Hub.

Argomenti

- Protezione dei dati in AWS Security Hub
- AWS Gestione delle identità e degli accessi per Security Hub
- Convalida della conformità per AWS Hub di sicurezza
- Resilienza in AWS Hub di sicurezza
- Sicurezza dell'infrastruttura in AWS Hub di sicurezza
- AWS Endpoint VPC di sicurezza e interfaccia (AWS PrivateLink)

Protezione dei dati in AWS Security Hub

Il modello di responsabilità AWS condivisa (modello di) si applica alla protezione dei dati in AWS Security Hub. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati . Per ulteriori informazioni sulla protezione dei dati in Europa, consulta il Centro generale sulla protezione dei dati (GDPR).

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e configurare singoli utenti con Centro identità AWS IAM o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.

- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Security Hub o altro Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Security Hub è un'offerta di servizi multi-tenant. Per proteggere i dati, Security Hub crittografa i dati inattivi e i dati in transito tra i servizi componenti.

Rifiuto esplicito all'utilizzo dei dati volto al miglioramento del servizio

> **Note**
>
> Questa pagina di documentazione è applicabile solo al AWS Security Hub avanzato lanciato il 2 dicembre 2025. Se sei un cliente del Security Hub originale (ora AWS Security Hub CSPM), l'utilizzo dei dati descritto di seguito si applicherà solo dopo aver abilitato il AWS Security Hub avanzato AWS .

Puoi scegliere di non utilizzare i tuoi dati (definiti come «Contenuto del Security Hub» nei termini del servizio Security Hub) per sviluppare e migliorare AWS Security Hub e altri servizi di AWS sicurezza utilizzando la politica di opt-out delle AWS organizzazioni. Puoi scegliere di annullare l'iscrizione anche se Security Hub attualmente non raccoglie tali Contenuti. Per ulteriori informazioni in merito, consulta le Policy di rifiuto dei servizi di IA nella Guida per l'utente di AWS Organizations .

> **Note**
>
> Per poter utilizzare la politica di opt-out, i tuoi AWS account devono essere gestiti centralmente dalle AWS organizzazioni. Se non hai già creato un'organizzazione per i tuoi AWS account, consulta Creazione e gestione di un'organizzazione nella Guida per l'AWS Organizations utente.

Il rifiuto esplicito ha gli effetti seguenti:

- Security Hub eliminerà i Contenuti raccolti e archiviati per scopi di miglioramento del servizio prima dell'eventuale rinuncia da parte dell'utente.
- Dopo la disattivazione, Security Hub non raccoglierà o archivierà più questi Contenuti per scopi di miglioramento del servizio.

La sezione seguente spiega come Security Hub gestirà i tuoi contenuti per il miglioramento del servizio.

AWS Utilizzo dei dati di Security Hub

Attualmente, AWS Security Hub non raccoglie o archivia alcun contenuto di Security Hub per scopi di miglioramento del servizio. Tuttavia, in futuro, Security Hub potrebbe raccogliere e utilizzare i risultati di sicurezza di terze parti che l'utente aggrega in Security Hub e in altre forme di contenuto di Security Hub (che Security Hub riceve dall'utente o da servizi a monte allo scopo di fornire funzionalità di Security Hub) per migliorare Security Hub e altre funzionalità dei servizi AWS di sicurezza.

La tua fiducia, la tua privacy e la sicurezza dei tuoi contenuti sono la nostra massima priorità. Se Security Hub inizierà a raccogliere i contenuti di Security Hub per scopi di miglioramento del servizio in futuro, questa pagina verrà aggiornata per riflettere tali modifiche e fornire dettagli sui dati raccolti e su come vengono utilizzati. Puoi disattivare questa raccolta di contenuti di Security Hub in qualsiasi momento utilizzando la politica di esclusione AWS delle organizzazioni descritta sopra. Per ulteriori informazioni sulle pratiche sulla privacy AWS dei dati, consulta le domande frequenti sulla privacy dei dati.

Riferimenti

Per procedure di opt-out simili in altri servizi AWS di sicurezza, consulta:

- Rinuncia all'utilizzo dei tuoi dati per il miglioramento del servizio nella Amazon GuardDuty User Guide.
- Rinuncia all'utilizzo dei tuoi dati per il miglioramento del servizio nella Guida per l'utente di Amazon Security Lake.

In che modo Security Hub utilizza i dati per fornire le funzionalità abilitate

Quando abiliti AWS Security Hub, vedrai un avviso che spiega che Security Hub può accedere e utilizzare i dati a cui ha già accesso per potenziare le funzionalità che scegli di abilitare. Questo avviso esiste perché Security Hub è progettato per crescere e migliorare nel tempo. Nuove funzionalità di rilevamento, correlazione e arricchimento vengono aggiunte su base continuativa e molte di queste si basano su dati (come risultati, dati di configurazione e altri contenuti o metadati) su cui Security Hub ha già visibilità come parte della configurazione esistente. Anziché chiederti di aderire ogni volta che introduciamo un modo per utilizzare i dati a cui hai già concesso l'accesso al Security Hub, questo avviso ti offre una visibilità chiara e anticipata su come può essere utilizzato tale accesso (ora e man mano che il servizio si evolve).

In pratica, ciò significa che l'attivazione di una funzionalità Security Hub è l'istruzione fornita a Security Hub di utilizzare i contenuti e i metadati pertinenti già a sua disposizione per fornire le funzionalità di tale funzionalità. Se una funzionalità che hai abilitato non sfrutta ancora appieno un particolare tipo di dati, la situazione potrebbe cambiare man mano che implementiamo i miglioramenti. Ad esempio, una funzionalità esistente potrebbe iniziare a incorporare un contesto aggiuntivo (come i segnali di criticità aziendale) per migliorare la precisione o fornirti informazioni più approfondite, senza costi aggiuntivi per te. Non sarà necessario intraprendere nuove azioni per rendere effettivi questi miglioramenti, poiché operano nell'ambito dell'accesso ai dati che hai già stabilito abilitando Security Hub e le sue funzionalità.

Questo approccio è progettato per migliorare la tua esperienza in quanto consente a Security Hub di migliorare continuamente il valore delle funzionalità che hai già attivato, senza creare problemi con ripetute richieste di consenso o configurazione per miglioramenti incrementali. Detto questo, hai il controllo: puoi rivedere, gestire o disabilitare le integrazioni e le funzionalità abilitate del Security Hub in qualsiasi momento tramite la console Security Hub, che determina a quali dati Security Hub può accedere e utilizzare in futuro.

AWS Gestione delle identità e degli accessi per Security Hub

AWS Identity and Access Management (IAM) è un modulo Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può

essere autenticato (accedere) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di Security Hub. IAM è un Servizio AWS programma che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso tramite policy
- Come funziona Security Hub con IAM
- Identity-based esempi di politiche per AWS Security Hub
- Service-linked ruoli per AWS Hub di sicurezza
- AWSpolitiche gestite per Security Hub
- Risoluzione dei problemi AWS Identità e accesso al Security Hub

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi AWS Identità e accesso al Security Hub)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta Come funziona Security Hub con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Identity-based esempi di politiche per AWS Security Hub)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali da una fonte di identità come Centro identità AWS IAM (IAM Identity Center), autenticazione Single Sign-on o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando ne crei uno Account AWS, inizi con un'identità di accesso chiamata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

È consigliabile richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità web o Directory Service che accede Servizi AWS utilizzando credenziali da una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, usa. Centro identità AWS IAM Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di Centro identità AWS IAM .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Come best practice, utilizza credenziali temporanee anziché utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella IAM User Guide.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un utente a un ruolo IAM (console) o chiamando un'operazione AWS API AWS CLI or. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un principale effettua una richiesta. La maggior parte delle policy sono archiviate AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Identity-based politiche

Identity-based le policy sono documenti relativi alle politiche di autorizzazione JSON che si allegano a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Identity-based le politiche possono essere politiche in linea (incorporate direttamente in una singola identità) o politiche gestite (politiche autonome associate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Resource-based politiche

Resource-based le policy sono documenti di policy JSON che alleghi a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Resource-based le policy sono policy in linea che si trovano in quel servizio. Non è possibile utilizzare le policy AWS gestite da IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): specifica il numero massimo di autorizzazioni per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di controllo delle risorse (RCP): imposta le autorizzazioni massime disponibili per le risorse degli account. Per ulteriori informazioni, consulta Policy di controllo delle risorse (RCP) nella Guida per l'utente di AWS Organizations .
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

Come funziona Security Hub con IAM

Prima di utilizzare AWS Identity and Access Management (IAM) per gestire l'accesso a AWS Security Hub, scopri quali funzionalità IAM sono disponibili per l'uso con Security Hub.

Funzionalità IAM che puoi utilizzare con AWS Security Hub

Funzionalità IAM	Supporto per Security Hub
Identity-based politiche	Sì
Resource-based politiche	No

Funzionalità IAM	Supporto per Security Hub
Operazioni di policy	Sì
Risorse relative alle policy	No
Chiavi di condizione delle policy	Sì
Liste di controllo accessi di rete (ACL)	No
Attribute-based controllo degli accessi (ABAC) — tag nelle politiche	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	No
Service-linked ruoli	Sì

Per una visione di alto livello di come Security Hub e altri Servizi AWS funzionano con la maggior parte delle funzionalità IAM, vedi Servizi AWS che funzionano con IAM nella IAM User Guide.

Identity-based politiche per Security Hub

Supporta le policy basate sull'identità: sì

Identity-based le policy sono documenti relativi alle politiche di autorizzazione JSON che è possibile allegare a un'identità, ad esempio un utente, un gruppo di utenti o un ruolo IAM. Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Security Hub supporta policy basate sull'identità. Per ulteriori informazioni, consulta Identity-based esempi di politiche per AWS Security Hub.

Resource-based politiche per Security Hub

Supporta le policy basate su risorse: no

Resource-based le policy sono documenti di policy JSON che alleghi a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Security Hub non supporta policy basate sulle risorse. Non è possibile allegare una policy IAM direttamente a una risorsa Security Hub.

Azioni politiche per Security Hub

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le politiche AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Le azioni relative alle policy in Security Hub utilizzano il seguente prefisso prima dell'azione:

```
securityhub:
```

Ad esempio, per concedere a un utente l'autorizzazione ad abilitare Security Hub, che è un'azione che corrisponde al `EnableSecurityHubV2` funzionamento dell'API Security Hub, includi l'`securityhub:EnableSecurityHubV2`azione nella relativa policy. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Security Hub definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

```
"Action": "securityhub:EnableSecurityHubV2"
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola. Ad esempio:

```
"Action": [
      "securityhub:EnableSecurityHubV2",
      "securityhub:CreateAutomationRuleV2"
```

È inoltre possibile specificare più azioni utilizzando caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Get`, includi la seguente azione:

```
"Action": "securityhub:Get*"
```

Tuttavia, è consigliabile definire policy in grado di seguire il principio del privilegio minimo. In altre parole, è necessario creare policy che includano solo le autorizzazioni necessarie per eseguire un'attività specifica.

Per un elenco delle azioni di Security Hub, vedere Azioni definite da AWS Security Hub nel riferimento all'autorizzazione del servizio. Per esempi di policy che specificano le azioni di Security Hub, vedereIdentity-based esempi di politiche per AWS Security Hub.

Risorse politiche per Security Hub

Supporta le risorse di policy: No

Gli amministratori possono utilizzare le politiche AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Security Hub definisce i seguenti tipi di risorse:

- Hub

- Prodotto
- Finding aggregator, noto anche come aggregatore interregionale
- Regola di automazione

È possibile specificare questi tipi di risorse nelle politiche utilizzando gli ARN.

Per un elenco dei tipi di risorse di Security Hub e la sintassi ARN per ciascuno di essi, vedere Resources Defined by AWS Security Hub nel Service Authorization Reference. Per informazioni sulle azioni che è possibile specificare per ogni tipo di risorsa, consulta Azioni definite da AWS Security Hub nel Service Authorization Reference. Per esempi di politiche che specificano le risorse, vedereIdentity-based esempi di politiche per AWS Security Hub.

Chiavi delle condizioni delle policy per Security Hub

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le politiche AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per vedere tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella IAM User Guide.

Per un elenco delle chiavi di condizione di Security Hub, consulta Chiavi di condizione per AWS Security Hub nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta Azioni definite da AWS Security Hub. Per esempi di policy che utilizzano chiavi di condizione, vedereIdentity-based esempi di politiche per AWS Security Hub.

Elenchi di controllo degli accessi (ACL) in Security Hub

Supporta le ACL: no

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Security Hub non supporta gli ACL, il che significa che non è possibile collegare un ACL a una risorsa Security Hub.

Attribute-based controllo degli accessi (ABAC) con Security Hub

Supporta ABAC (tag nelle policy): sì

Attribute-based il controllo degli accessi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. È possibile allegare tag alle entità e alle AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Puoi allegare tag alle risorse di Security Hub. Puoi anche controllare l'accesso alle risorse fornendo le informazioni sui tag nell'`Condition`elemento di una policy.

Per informazioni sulla codifica delle risorse di Security Hub, vedereTaggare le risorse del Security Hub. Per un esempio di policy basata sull'identità che controlla l'accesso a una risorsa in base ai tag, vedi. Identity-based esempi di politiche per AWS Security Hub

Utilizzo di credenziali temporanee con Security Hub

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. È possibile ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come o. AssumeRole GetFederationToken

Security Hub supporta l'uso di credenziali temporanee.

Inoltra le sessioni di accesso per Security Hub

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso diretto (FAS) utilizzano le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi a valle. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ad esempio, Security Hub effettua il downstream delle richieste FAS Servizi AWS quando si integra Security Hub con AWS Organizations e quando si designa l'account amministratore delegato di Security Hub per un'organizzazione in Organizations.

Per altre attività, Security Hub utilizza un ruolo collegato al servizio per eseguire azioni per conto dell'utente. Per informazioni dettagliate su questo ruolo, consulta. Service-linked ruoli per AWS Hub di sicurezza

Ruoli di servizio per Security Hub

Security Hub non assume né utilizza ruoli di servizio. Per eseguire azioni per conto dell'utente, Security Hub utilizza un ruolo collegato al servizio. Per informazioni dettagliate su questo ruolo, consulta. Service-linked ruoli per AWS Hub di sicurezza

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio può creare problemi operativi con l'utilizzo di Security Hub. Modifica i ruoli di servizio solo quando Security Hub fornisce indicazioni in tal senso.

Service-linked ruoli per Security Hub

Supporta i ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo di eseguire un'azione per conto dell'utente. Service-linked i ruoli vengono

visualizzati nell'utente Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Security Hub utilizza un ruolo collegato al servizio per eseguire azioni per conto dell'utente. Per informazioni dettagliate su questo ruolo, consulta. Service-linked ruoli per AWS Hub di sicurezza

Identity-based esempi di politiche per AWS Security Hub

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare AWS Security Hub risorse. Inoltre, non possono eseguire attività utilizzando l' AWS API Console di gestione AWS AWS CLI, o. Un amministratore deve creare le policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore devi quindi collegare queste policy a utenti o gruppi che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente IAM.

Argomenti

- Best practice delle policy
- Utilizzo della console Security Hub
- Esempio: consentire agli utenti di visualizzare le loro autorizzazioni
- Esempio: consenti agli utenti di visualizzare i risultati
- Esempio: consentire agli utenti di creare e gestire regole di automazione

Best practice delle policy

Identity-based i criteri determinano se qualcuno può creare, accedere o eliminare le risorse del Security Hub nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti

specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Security Hub

Per accedere alla AWS Security Hub console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse del Security Hub presenti nel tuo Account AWS. Se si crea una politica basata sull'identità più restrittiva delle autorizzazioni minime richieste, la console non funzionerà come previsto per le entità (utenti o ruoli) che applicano tale politica.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso o l'API. AWS CLI AWS Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che tali utenti e ruoli possano utilizzare la console Security Hub, allega anche la seguente politica AWS gestita all'entità. Per ulteriori informazioni, consulta la sezione Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Esempio: consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l' AWS CLI API o. 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": "*"
        }
    ]
}
```

Esempio: consenti agli utenti di visualizzare i risultati

Questo esempio mostra come è possibile creare una policy IAM che consenta a un utente di visualizzare i risultati del Security Hub.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
```

```
                "securityhub:GetFindingsV2"
            ],
            "Resource": "*"
        }
    ]
}
```

Esempio: consentire agli utenti di creare e gestire regole di automazione

Questo esempio mostra come è possibile creare una policy IAM che consenta a un utente di creare, visualizzare, aggiornare ed eliminare le regole di automazione del Security Hub. Affinché questa policy IAM funzioni, l'utente deve essere un amministratore del Security Hub. Per limitare le autorizzazioni, ad esempio per consentire a un utente di visualizzare solo le regole di automazione, puoi rimuovere le autorizzazioni di creazione, aggiornamento ed eliminazione.

```
{
    "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 ruoli per AWS Hub di sicurezza

AWS Security Hub utilizza un ruolo collegato al servizio AWS Identity and Access Management (IAM) denominato. `AWSServiceRoleForSecurityHubV2` Questo ruolo collegato ai servizi è un ruolo IAM collegato direttamente a Security Hub. È predefinito da Security Hub e include tutte le autorizzazioni necessarie a Security Hub per chiamare altre AWS risorse Servizi AWS e monitorare per tuo conto. Security Hub utilizza questo ruolo collegato al servizio in tutti i luoghi in Regioni AWS cui Security Hub è disponibile.

Un ruolo collegato al servizio semplifica la configurazione di Security Hub perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Security Hub definisce le autorizzazioni del suo ruolo collegato ai servizi e, se non diversamente definito, solo Security Hub può assumere il ruolo. Le autorizzazioni definite includono la politica di fiducia e la politica delle autorizzazioni e non è possibile allegare tale politica di autorizzazioni a nessun'altra entità IAM.

Per esaminare i dettagli del ruolo collegato al servizio, puoi utilizzare la console Security Hub. Nel pannello di navigazione, scegli Generale in Impostazioni. Quindi, nella sezione Autorizzazioni di servizio, scegli Visualizza le autorizzazioni del servizio.

Puoi eliminare il ruolo collegato al servizio Security Hub solo dopo aver disabilitato Security Hub in tutte le regioni in cui è abilitato. Questo protegge le tue risorse di Security Hub perché non puoi rimuovere inavvertitamente le autorizzazioni per accedervi.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta i AWS servizi che funzionano con IAM nella IAM User Guide e individua i servizi con Sì nella colonna dei ruoli. Service-linked Scegli un Sì con un link per consultare la documentazione sui ruoli collegati al servizio per quel servizio.

Argomenti

- Service-linked autorizzazioni di ruolo per Security Hub
- Creazione di un ruolo collegato ai servizi per Security Hub
- Modifica di un ruolo collegato al servizio per Security Hub
- Eliminazione di un ruolo collegato al servizio per Security Hub

Service-linked autorizzazioni di ruolo per Security Hub

Security Hub utilizza il ruolo collegato al servizio denominato. `AWSServiceRoleForSecurityHubV2` È un ruolo collegato al servizio necessario per consentire a AWS Security Hub di accedere alle tue risorse. Questo ruolo collegato ai servizi consente a Security Hub di eseguire attività quali ricevere risultati da altri Servizi AWS e configurare l' AWS Config infrastruttura necessaria per eseguire i controlli di sicurezza per i controlli. Ai fini dell'assunzione del ruolo `AWSServiceRoleForSecurityHubV2`, il ruolo collegato ai servizi `securityhub.amazonaws.com`considera attendibile il servizio.

Il ruolo collegato ai servizi `AWSServiceRoleForSecurityHubV2` utilizza la policy gestita `AWSSecurityHubV2ServiceRolePolicy`.

È necessario concedere le autorizzazioni per consentire a un'identità IAM (ad esempio un ruolo, un gruppo o un utente) di creare, modificare o eliminare un ruolo collegato al servizio. `AWSServiceRoleForSecurityHubV2`Affinché il ruolo collegato al servizio venga creato correttamente, l'identità IAM utilizzata per accedere a Security Hub deve disporre delle autorizzazioni richieste. Per concedere le autorizzazioni richieste, collega la seguente policy all'identità IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
```

```
}
```

Creazione di un ruolo collegato ai servizi per Security Hub

Il ruolo `AWSServiceRoleForSecurityHubV2` collegato al servizio viene creato automaticamente quando si abilita Security Hub per la prima volta o si abilita Security Hub in una regione in cui non era abilitato in precedenza. Puoi anche creare il ruolo `AWSServiceRoleForSecurityHubV2` collegato al servizio manualmente utilizzando la console IAM, l'IAM CLI o l'API IAM. Per ulteriori informazioni sulla creazione manuale del ruolo, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM.

> **Important**
>
> Il ruolo collegato al servizio creato per un account amministratore di Security Hub non si applica agli account membri di Security Hub associati.

Modifica di un ruolo collegato al servizio per Security Hub

Security Hub non consente di modificare il ruolo collegato al `AWSServiceRoleForSecurityHubV2` servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché potrebbero farvi riferimento varie entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Security Hub

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, elimina il ruolo. In questo modo, non hai un'entità inutilizzata che non sia monitorata o gestita attivamente.

Quando disabiliti Security Hub, Security Hub non elimina automaticamente il ruolo `AWSServiceRoleForSecurityHubV2` collegato al servizio per te. Se abiliti nuovamente Security Hub, il servizio può ricominciare a utilizzare il ruolo collegato al servizio esistente. Se non è più necessario utilizzare Security Hub, è possibile eliminare manualmente il ruolo collegato al servizio.

> **Important**
>
> Prima di eliminare il ruolo `AWSServiceRoleForSecurityHubV2` collegato al servizio, devi prima disabilitare Security Hub in tutte le regioni in cui è abilitato. Per ulteriori informazioni, consulta Disattivazione di Security Hub. Se Security Hub non è disabilitato quando si tenta di eliminare il ruolo collegato al servizio, l'eliminazione non riesce.

Per eliminare il ruolo `AWSServiceRoleForSecurityHubV2` collegato al servizio, puoi utilizzare la console IAM, l'IAM CLI o l'API IAM. Per ulteriori informazioni, consultare Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

AWSpolitiche gestite per Security Hub

Una policy AWS gestita è una policy autonoma creata e amministrata da. AWS AWSle politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWSè più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

AWSpolitica gestita: AWSSecurityHubFullAccess

È possibile allegare la policy `AWSSecurityHubFullAccess` alle identità IAM.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo principale a tutte le azioni del Security Hub. Questa politica deve essere associata a un principale prima che quest'ultimo abiliti manualmente Security Hub per il proprio account. Ad esempio, i responsabili con queste autorizzazioni possono sia visualizzare che aggiornare lo stato dei risultati. Possono anche

configurare approfondimenti personalizzati, abilitare integrazioni e abilitare e disabilitare standard e controlli. I responsabili di un account amministratore possono anche gestire gli account dei membri.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `securityhub`— Consente ai responsabili l'accesso completo a tutte le azioni del Security Hub.
- `guardduty`— Consente ai responsabili di ottenere informazioni sullo stato dell'account in Amazon GuardDuty.
- `iam`— Consente ai responsabili di creare un ruolo collegato ai servizi per Security Hub.
- `inspector`— Consente ai responsabili di ottenere informazioni sullo stato dell'account in Amazon Inspector.
- `pricing`— Consente ai committenti di ottenere un listino prezzi e prodotti. Servizi AWS

Per esaminare le autorizzazioni relative a questa politica, consulta AWSSecurityHubFullAccessla AWSManaged Policy Reference Guide.

AWSpolitica gestita: AWSSecurityHubReadOnlyAccess

È possibile allegare la policy `AWSSecurityHubReadOnlyAccess` alle identità IAM.

Questa politica concede autorizzazioni di sola lettura che consentono agli utenti di visualizzare le informazioni in Security Hub. I responsabili a cui è allegata questa politica non possono effettuare aggiornamenti in Security Hub. Ad esempio, i responsabili con queste autorizzazioni possono visualizzare l'elenco dei risultati associati al proprio account, ma non possono modificare lo stato di un risultato. Possono visualizzare i risultati degli approfondimenti, ma non possono creare o configurare approfondimenti personalizzati. Non possono configurare controlli o integrazioni di prodotti.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `securityhub`— Consente agli utenti di eseguire azioni che restituiscono un elenco di elementi o dettagli su un elemento. Ciò include le operazioni API che iniziano con `GetList`, o`Describe`.

Per esaminare le autorizzazioni relative a questa policy, consulta AWSSecurityHubReadOnlyAccessla AWSManaged Policy Reference Guide.

AWSpolitica gestita: AWSSecurityHubOrganizationsAccess

È possibile allegare la policy `AWSSecurityHubOrganizationsAccess` alle identità IAM.

Questa politica concede le autorizzazioni amministrative per abilitare e gestire Security Hub per un'organizzazione in. AWS Organizations Le autorizzazioni per questa politica consentono all'account di gestione dell'organizzazione di designare l'account amministratore delegato per Security Hub. Consentono inoltre all'account amministratore delegato di abilitare gli account dell'organizzazione come account membro.

Questa politica fornisce solo le autorizzazioni per. AWS Organizations L'account di gestione dell'organizzazione e l'account amministratore delegato richiedono inoltre le autorizzazioni per le azioni associate. Queste autorizzazioni possono essere concesse utilizzando la politica gestita`AWSSecurityHubFullAccess`.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `organizations:ListAccounts`— Consente ai responsabili di recuperare l'elenco degli account che fanno parte di un'organizzazione.
- `organizations:DescribeOrganization`— Consente ai dirigenti di recuperare informazioni sull'organizzazione.
- `organizations:ListRoots`— Consente ai dirigenti di elencare la radice di un'organizzazione.
- `organizations:ListDelegatedAdministrators`— Consente ai dirigenti di elencare l'amministratore delegato di un'organizzazione.
- `organizations:ListAWSServiceAccessForOrganization`— Consente ai dirigenti di elencare le informazioni utilizzate da un'Servizi AWSorganizzazione.
- `organizations:ListOrganizationalUnitsForParent`— Consente ai responsabili di elencare le unità organizzative (OU) secondarie di un'unità organizzativa principale.
- `organizations:ListAccountsForParent`— Consente ai responsabili di elencare gli account secondari di un'unità organizzativa principale.
- `organizations:ListParents`— Elenca le unità organizzative o principali (OU) che fungono da elemento principale dell'unità organizzativa o dell'account figlio specificato.
- `organizations:DescribeAccount`: consente ai principali di recuperare informazioni su un account nell'organizzazione.

- `organizations:DescribeOrganizationalUnit`— Consente ai responsabili di recuperare informazioni su un'unità organizzativa all'interno dell'organizzazione.
- `organizations:ListPolicies`— Recupera l'elenco di tutte le politiche di un'organizzazione di un tipo specificato.
- `organizations:ListPoliciesForTarget`— Elenca le politiche direttamente collegate alla radice, all'unità organizzativa (OU) o all'account di destinazione specificati.
- `organizations:ListTargetsForPolicy`— Elenca tutte le radici, le unità organizzative (OU) e gli account a cui è associata la politica specificata.
- `organizations:EnableAWSServiceAccess`— Consente ai presidi di abilitare l'integrazione con Organizations.
- `organizations:RegisterDelegatedAdministrator`— Consente ai responsabili di designare l'account amministratore delegato.
- `organizations:DeregisterDelegatedAdministrator`— Consente ai responsabili di rimuovere l'account di amministratore delegato.
- `organizations:DescribePolicy`— Recupera informazioni su una politica.
- `organizations:DescribeEffectivePolicy`— Restituisce il contenuto della politica effettiva per il tipo di politica e l'account specificati.
- `organizations:CreatePolicy`— Crea una politica di un tipo specifico che è possibile allegare a una radice, a un'unità organizzativa (OU) o a un AWS account individuale.
- `organizations:UpdatePolicy`— Aggiorna una politica esistente con un nuovo nome, descrizione o contenuto.
- `organizations:DeletePolicy`— Elimina la politica specificata dall'organizzazione.
- `organizations:AttachPolicy`— Associa una policy a una root, a un'unità organizzativa (OU) o a un account individuale.
- `organizations:DetachPolicy`— Scollega una politica da una radice, un'unità organizzativa (OU) o un account di destinazione.
- `organizations:EnablePolicyType`— Abilita un tipo di policy in una radice.
- `organizations:DisablePolicyType`— Disattiva un tipo di politica organizzativa in una radice.
- `organizations:TagResource`— Aggiunge uno o più tag a una risorsa specificata.
- `organizations:UntagResource`— Rimuove tutti i tag con le chiavi specificate da una risorsa specificata.
- `organizations:ListTagsForResource`— Elenca i tag allegati a una risorsa specificata.

Per esaminare le autorizzazioni relative a questa policy, consulta AWSSecurityHubOrganizationsAccessla AWSManaged Policy Reference Guide.

AWSpolitica gestita: AWSSecurityHubV2ServiceRolePolicy

Questa politica consente a Security Hub di gestire AWS Config le regole e le risorse del Security Hub per l'organizzazione e per conto dell'utente. Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non è possibile allegare la policy alle identità IAM. Per ulteriori informazioni, consulta the section called "Service-linked ruoli".

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `access-analyzer`— Crea ed elimina IAM Access Analyzer collegati ai servizi quando i clienti abilitano o disabilitano Security Hub, elenca gli analizzatori per verificare che lo stato dell'analizzatore sia coerente con lo stato di abilitazione e genera e recupera consigli sulle policy per i risultati di accesso non utilizzati.
- `cloudwatch`— Recupera i dati delle metriche per supportare le funzionalità di misurazione per le risorse del Security Hub e le metriche sullo stato del connettore.
- `config`— Gestione dei registratori di configurazione collegati ai servizi e dei registratori di configurazione collegati ai servizi di terze parti per le risorse Security Hub, incluso il supporto per i registratori Config globali. Elenca i registratori di configurazione e ottieni informazioni sui connettori per supportare integrazioni cloud di terze parti.
- `ecr`— Recupera informazioni sulle immagini e sugli archivi di Amazon Elastic Container Registry per supportare le funzionalità di misurazione.
- `iam`— Crea i seguenti ruoli collegati al servizio:AWS Config, IAM Access Analyzer nell'account del cliente e Amazon Inspector per la scansione di terze parti. Recupera le informazioni sull'account per supportare le funzionalità di misurazione. Recupera le policy IAM esistenti in modo che i clienti possano visualizzare un confronto tra la loro politica attuale e la soluzione sostitutiva con privilegi minimi consigliata.
- `inspector2`— Crea, aggiorna, elimina ed elenca i connettori Amazon Inspector e le configurazioni di scansione dei connettori per supportare integrazioni cloud di terze parti.
- `lambda`— Recupera le informazioni sulle AWS Lambda funzioni per supportare le funzionalità di misurazione.
- `organizations`— Recupera informazioni sull'account e sull'unità organizzativa (OU) di un'organizzazione.

- `securityhub`— Gestire la configurazione del Security Hub. Crea, aggiorna ed elimina i connettori Security Hub per supportare integrazioni cloud di terze parti.
- `sts`— Ottieni token di identità web per la federazione delle identità in uscita per supportare integrazioni cloud di terze parti.
- `tag`— Recupera informazioni sui tag delle risorse.

Per esaminare le autorizzazioni relative a questa politica, consulta AWSSecurityHubV2ServiceRolePolicyla AWSManaged Policy Reference Guide.

Aggiornamenti del Security Hub aAWSpolicy gestite

La tabella seguente fornisce dettagli sugli aggiornamenti alle politiche AWS gestite per AWS Security Hub da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sugli aggiornamenti delle politiche, iscriviti al feed RSS nella pagina della cronologia dei documenti di Security Hub.

Modifica	Descrizione	Data
AWSSecurityHubV2ServiceRolePolicy— Politica aggiornata	Security Hub ha aggiornato la politica per supportare le integrazioni di terze parti. L'aggiornamento aggiunge le seguenti autorizzazioni: gestione di registratori di configurazione di terze parti, creazione e gestione di connettori Security Hub e Amazon Inspector, recupero dei parametri di integrità dei connettori, CloudWatch creazione del ruolo collegato al servizio Amazon Inspector per la scansione di terze parti e ottenimento di token di	30 giugno 2026

Modifica	Descrizione	Data
	identità Web per la federazione.	
AWSSecurityHubV2ServiceRolePolicy— Politica aggiornata	Security Hub ha aggiornato la policy per aggiungere le autorizzazioni IAM Access Analyzer. L'aggiornamento consente a Security Hub di creare e gestire analizzatori gestiti dai servizi, elencare gli analizzatori per verificare che la configurazione dell'analizzatore sia coerente con lo stato di abilitazione, generare e recuperare consigli sulle policy per i risultati di accesso non utilizzati e recuperare le politiche IAM per la visualizzazione delle raccomandazioni.	10 maggio 2026
AWSSecurityHubOrganizationsAccess— Politica aggiornata	Security Hub ha aggiornato la politica per aggiungere autorizzazioni per descrivere le politiche delle risorse per supportare le funzionalità di Security Hub. Security Hub è in versione di anteprima ed è soggetto a modifiche.	12 novembre 2025

Modifica	Descrizione	Data
AWSSecurityHubFullAccess— Politica aggiornata	Security Hub ha aggiornato la policy per aggiungere funzionalità di gestione GuardDuty, Amazon Inspector e gestione degli account per supportare le funzionalità di Security Hub. Security Hub è in versione di anteprima ed è soggetto a modifiche.	17 novembre 2025
AWSSecurityHubV2ServiceRolePolicy— Politica aggiornata	Security Hub ha aggiornato la policy per aggiungere funzionalità di misurazione per Amazon Elastic Container Registry AWS Lambda CloudWatch, Amazon e AWS Identity and Access Management per supportare le funzionalità di Security Hub. L'aggiornamento ha inoltre aggiunto il supporto per i AWS Config registratori globali. Security Hub è in versione di anteprima ed è soggetto a modifiche.	5 novembre 2025
AWSSecurityHubOrganizationsAccess: aggiornamento di una policy esistente	Security Hub ha aggiunto nuove autorizzazioni alla policy. Le autorizzazioni consentono alla direzione dell'organizzazione di abilitare e gestire Security Hub e Security Hub CSPM per un'organizzazione.	17 giugno 2025

Modifica	Descrizione	Data
AWSSecurityHubFullAccess: aggiornamento di una policy esistente	Security Hub CSPM ha aggiunto nuove autorizzazioni che consentono ai responsabili di creare un ruolo collegato al servizio per Security Hub.	17 giugno 2025
AWSSecurityHubV2ServiceRolePolicy: nuova policy	Security Hub ha aggiunto una nuova policy per consentire a Security Hub di gestire AWS Config le regole e le risorse del Security Hub per l'organizzazione di un cliente e per conto del cliente. Security Hub è in versione di anteprima ed è soggetto a modifiche.	17 giugno 2025
AWSSecurityHubFullAccess— Aggiornamento a una politica esistente	Security Hub CSPM ha aggiornato la politica per ottenere dettagli sui prezzi Servizi AWS e sui prodotti.	24 aprile 2024
AWSSecurityHubReadOnlyAccess— Aggiornamento a una politica esistente	Security Hub CSPM ha aggiornato questa politica gestita aggiungendo un `Sid` campo.	22 febbraio 2024
AWSSecurityHubFullAccess— Aggiornamento a una politica esistente	Security Hub CSPM ha aggiornato la policy in modo da determinare se Amazon GuardDuty e Amazon Inspector sono abilitati in un account. Questo aiuta i clienti a riunire informazioni relative alla sicurezza provenienti da più fonti. Servizi AWS	16 novembre 2023

Modifica	Descrizione	Data
AWSSecurityHubOrganizationsAccess— Aggiornamento a una politica esistente	Security Hub CSPM ha aggiornato la politica per concedere autorizzazioni aggiuntive per consentire l'accesso in sola lettura alle funzionalità di amministratore delegato. AWS Organizations Ciò include dettagli come la radice, le unità organizzative (OU), gli account, la struttura organizzativa e l'accesso al servizio.	16 novembre 2023
AWSSecurityHubOrganizationsAccess— Nuova politica	Security Hub CSPM ha aggiunto una nuova politica che concede le autorizzazioni necessarie per l'integrazione del Security Hub CSPM con Organizations.	15 marzo 2021
Security Hub CSPM ha iniziato a tracciare le modifiche	Security Hub CSPM ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	15 marzo 2021

Risoluzione dei problemi AWS Identità e accesso al Security Hub

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare lavorando con AWS Security Hub e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Security Hub
- Non sono autorizzato a eseguire iam: PassRole
- Desidero un accesso programmatico a Security Hub

- Sono un amministratore e voglio consentire ad altri di accedere a Security Hub
- Voglio consentire l'accesso a persone esterne al mio Account AWS per accedere alle mie risorse Security Hub

Non sono autorizzato a eseguire un'azione in Security Hub

Se ti Console di gestione AWS dice che non sei autorizzato a eseguire un'azione, devi contattare il tuo amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` tenta di utilizzare la console per visualizzare i dettagli su a *`widget`* ma non dispone `securityhub:`*`GetWidget`* delle autorizzazioni.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

In questo caso, Mateo chiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *`my-example-widget`* mediante l'operazione `securityhub:`*`GetWidget`*.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue policy devono essere aggiornate per consentirti di passare un ruolo a Security Hub.

Alcune Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Security Hub. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Desidero un accesso programmatico a Security Hub

Gli utenti hanno bisogno di un accesso programmatico se vogliono interagire con l' AWS esterno. Console di gestione AWS Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Consigliato) Utilizza le credenziali della console come credenziali temporanee per firmare richieste programma tiche a AWS SDK o AWS CLI API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per saperne di più AWS CLI, consulta Login for AWS local development nella Guida per l'utente. AWS Command Line Interface • Per AWS gli SDK, consulta Login for AWS local development nella Guida di riferimento per AWS SDK and Tools.
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Usa le credenziali temporane e per firmare le richieste programmatiche agli AWS SDK o alle AWS CLI API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per saperne di più AWS CLI, consulta Configura zione dell'uso Centro identità AWS IAM nella Guida AWS CLI per l'utente. AWS Command Line Interface

Quale utente necessita dell'accesso programmatico?	Per	Come
		• Per AWS SDK, strumenti e AWS API, consulta l'autenti cazione IAM Identity Center nella Guida di riferimento per AWS SDK e strumenti.
IAM	Usa le credenziali temporane e per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS	Seguendo le istruzioni in Uso delle credenziali temporanee con le AWS risorse nella IAM User Guide.
IAM	(Non consigliato) Usa le credenziali a lungo termine per firmare richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per saperne di più AWS CLI, consulta Autentica zione tramite credenziali utente IAM nella Guida per l'utente. AWS Command Line Interface • Per AWS SDK e strumenti , consulta Autenticare utilizzando credenziali a lungo termine nella Guida di riferimento per SDK e strumenti. AWS • Per le AWS API, consulta Gestire le chiavi di accesso per gli utenti IAM nella IAM User Guide.

Sono un amministratore e voglio consentire ad altri di accedere a Security Hub

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- Utenti e gruppi in Centro identità AWS IAM:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di Centro identità AWS IAM .

- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Create a role for a third-party identity provider (federation) della Guida per l'utente IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina Create a role for an IAM user della Guida per l'utente IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

Voglio consentire l'accesso a persone esterne al mio Account AWS per accedere alle mie risorse Security Hub

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizzare tali policy per concedere alle persone l'accesso alle proprie risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Security Hub supporta queste funzionalità, consultaCome funziona Security Hub con IAM.
- Per sapere come fornire l'accesso alle risorse di Account AWS cui sei proprietario, consulta Fornire l'accesso a un utente IAM in un altro Account AWS utente di tua proprietà nella IAM User Guide.
- Per sapere come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a risorse Account AWS di proprietà di terzi nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Convalida della conformità per AWS Hub di sicurezza

La nostra nuova esperienza AWS di iscrizione non è progettata per carichi di lavoro regolamentati. Se stai utilizzando la nostra nuova esperienza di AWS registrazione, ma desideri utilizzarla AWS per carichi di lavoro regolamentati, puoi iscriverti a AWS (avanzato) o attivare funzionalità avanzate per il tuo ambiente. AWS

Per sapere se un Servizio AWS rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program e scegli il programma di conformità che ti interessa. Per informazioni generali, vedere Programmi di AWS conformità Programmi di

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, vedere Scaricamento dei report in AWS Artifact .

La responsabilità dell'utente in materia di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità dell'utente in materia di conformità durante l'utilizzo Servizi AWS, consulta AWS la Documentazione sulla sicurezza.

Resilienza in AWS Hub di sicurezza

L'infrastruttura AWS globale è costruita attorno alle zone Regioni AWS di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità Regioni AWS e sulle zone di disponibilità, consulta AWS Global Infrastructure.

Sicurezza dell'infrastruttura in AWS Hub di sicurezza

In quanto servizio gestito, AWS Security Hub è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi le chiamate API AWS pubblicate per accedere a Security Hub attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di crittografia con Perfect Forward Secrecy (PFS) come DHE (Ephemeral) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

AWS Endpoint VPC di sicurezza e interfaccia (AWS PrivateLink)

Puoi stabilire una connessione privata tra il tuo VPC e AWS Security Hub creando un endpoint VPC di interfaccia. Gli endpoint di interfaccia sono basati su una tecnologia che consente di accedere privatamente alle API di Security Hub senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione Direct Connect. AWS PrivateLink AWS Le istanze del tuo VPC non necessitano di indirizzi IP pubblici per comunicare con le API di Security Hub. Il traffico tra il tuo VPC e Security Hub non esce dalla rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più interfacce di rete elastiche nelle sottoreti. Per ulteriori informazioni, consulta Accedere a un endpoint VPC Servizio AWS tramite interfaccia nella Amazon Virtual Private Cloud Guide.

Considerazioni sugli endpoint VPC di Security Hub

Prima di configurare un endpoint VPC di interfaccia per Security Hub, assicurati di esaminare i prerequisiti e le altre informazioni contenute nella Amazon Virtual Private Cloud Guide. https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html

Security Hub supporta l'esecuzione di chiamate a tutte le azioni API dal tuo VPC.

Creazione di un endpoint VPC di interfaccia per Security Hub

Puoi creare un endpoint VPC per il servizio Security Hub utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta Create a VPC endpoint nella Amazon Virtual Private Cloud Guide.

Crea un endpoint VPC per Security Hub utilizzando il seguente nome di servizio:

`com.amazonaws.`*`region`*`.securityhub`

*`region`*Dov'è il codice regionale applicabile. Regione AWS

Se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API a Security Hub utilizzando il nome DNS predefinito per la regione, `securityhub.us-east-1.amazonaws.com` ad esempio per la regione Stati Uniti orientali (Virginia settentrionale).

Creazione di una policy sugli endpoint VPC per Security Hub

Puoi allegare una policy sugli endpoint al tuo endpoint VPC che controlli l'accesso a Security Hub. La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire azioni.

Per ulteriori informazioni, consulta Controllare l'accesso agli endpoint VPC utilizzando le policy per gli endpoint nella Amazon Virtual Private Cloud Guide.

Esempio: policy sugli endpoint VPC per le azioni di Security Hub

Di seguito è riportato un esempio di policy sugli endpoint per Security Hub. Se collegata a un endpoint, questa policy consente l'accesso alle azioni elencate di Security Hub a tutti i principali su tutte le risorse.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Sottoreti condivise

Non puoi creare, descrivere, modificare o eliminare gli endpoint VPC nelle sottoreti condivise con te. Tuttavia, puoi utilizzare gli endpoint VPC in sottoreti condivise con te. Per informazioni sulla condivisione VPC, consulta Condividi le tue sottoreti VPC con altri account nella Amazon Virtual Private Cloud Guide.

Registrazione delle chiamate API Security Hub con CloudTrail

è integrato con AWS CloudTrail un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Security Hub. CloudTrail acquisisce le chiamate API per Security Hub come eventi. Le chiamate acquisite includono le chiamate dalla console Security Hub e le chiamate in codice alle operazioni dell'API Security Hub. Se crei un percorso, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Security Hub. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti sulla CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni CloudTrail raccolte, è possibile determinare la richiesta effettuata a Security Hub, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per saperne di più CloudTrail, incluso come configurarlo e abilitarlo, consulta la Guida per l'AWS CloudTrail utente.

Informazioni su Security Hub in CloudTrail

CloudTrail è abilitato sul tuo Account AWS computer quando crei l'account. Quando si verifica un'attività di evento supportata in Security Hub, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account . Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo account, inclusi gli eventi per Security Hub, crea un percorso. Un percorso consente di CloudTrail inviare file di registro a un bucket Amazon S3. Per impostazione predefinita, quando crei un trail nella console, il trail si applica a tutte le regioni AWS . Il percorso registra gli eventi provenienti da tutte le regioni della AWS partizione e invia i file di registro al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati degli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso

- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Security Hub supporta la registrazione di tutte le azioni dell'API Security Hub come eventi nei CloudTrail registri. Per visualizzare un elenco delle operazioni di Security Hub, consulta il Security Hub API Reference.

Quando viene registrata l'attività per le seguenti azioni CloudTrail, il valore per `responseElements` è impostato su. `null` Ciò garantisce che le informazioni sensibili non siano incluse nei CloudTrail registri.

- `GetFindingsV2`

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM)
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Esempio: voci del file di registro di Security Hub

Un trail è una configurazione che consente l'invio di eventi come file di registro a un bucket Amazon S3 specificato. CloudTrail i file di log contengono una o più voci di registro. Un evento rappresenta una singola richiesta da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreateAutomationRuleV2`azione. In questo esempio, `TestAutomationRule` viene creata

una regola di automazione denominata. `Account ID`Gli attributi `Severity` e sono specificati come criteri. Quando la regola viene soddisfatta, `Severity` viene aggiornata a Alta. Per ulteriori informazioni sulle regole di automazione, vedereRegole di automazione 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"
}
```

Introduzione a AWS Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) ti offre una visione completa del tuo stato di sicurezza AWS e ti aiuta a valutare il tuo AWS ambiente rispetto agli standard e alle migliori pratiche del settore della sicurezza.

AWS Security Hub CSPM raccoglie dati sulla sicurezza su Account AWS prodotti di terze parti supportati e ti aiuta ad analizzare le tendenze della sicurezza e identificare i problemi di sicurezza con la massima priorità. Servizi AWS

Per aiutarti a gestire lo stato di sicurezza della tua organizzazione, Security Hub CSPM supporta diversi standard di sicurezza. Questi includono lo standard AWS Foundational Security Best Practices (FSBP) sviluppato da AWS e framework di conformità esterni come il Center for Internet Security (CIS), il Payment Card Industry Data Security Standard (PCI DSS) e il National Institute of Standards and Technology (NIST). Ogni standard include diversi controlli di sicurezza, ognuno dei quali rappresenta una best practice di sicurezza. Security Hub CSPM esegue controlli rispetto ai controlli di sicurezza e genera risultati di controllo per aiutarti a valutare la tua conformità rispetto alle migliori pratiche di sicurezza.

Oltre a generare risultati di controllo, Security Hub CSPM riceve anche i risultati da altri, Servizi AWS come Amazon, Amazon GuardDuty Inspector e Amazon Macie, e da prodotti di terze parti supportati. Questo ti offre un'unica finestra di controllo per una serie di problemi relativi alla sicurezza. Puoi anche inviare i risultati CSPM di Security Hub ad altri Servizi AWS prodotti di terze parti supportati.

Security Hub CSPM offre funzionalità di automazione che aiutano a valutare e risolvere i problemi di sicurezza. Ad esempio, è possibile utilizzare le regole di automazione per aggiornare automaticamente i risultati critici quando un controllo di sicurezza fallisce. Puoi anche sfruttare l'integrazione con Amazon EventBridge per attivare risposte automatiche a risultati specifici.

Argomenti

- Vantaggi del Security Hub CSPM
- Accesso a Security Hub CSPM
- Servizi correlati
- Versione di prova gratuita e prezzi di Security Hub CSPM
- Concetti e terminologia in Security Hub CSPM
- Abilitazione di Security Hub CSPM

- Gestione degli account di amministratore e membro in Security Hub CSPM
- Comprendere l'aggregazione interregionale in Security Hub CSPM
- Comprensione degli standard di sicurezza in Security Hub CSPM
- Comprendere i controlli di sicurezza in Security Hub CSPM
- Comprendere le integrazioni in Security Hub CSPM
- Integrazione del Security Hub CSPM con Microsoft Azure
- Creazione e aggiornamento dei risultati in Security Hub CSPM
- Visualizzazione degli approfondimenti in Security Hub CSPM
- Modifica e azione automatica dei risultati in Security Hub CSPM
- Utilizzo della dashboard in Security Hub CSPM
- Limiti regionali per Security Hub CSPM
- Creazione di risorse CSPM Security Hub con CloudFormation
- Iscrizione agli annunci CSPM di Security Hub con Amazon SNS
- Disattivazione del Security Hub CSPM
- Sicurezza in AWS Security Hub CSPM
- Registrazione delle chiamate API Security Hub con CloudTrail

Vantaggi del Security Hub CSPM

Ecco alcuni dei modi principali in cui Security Hub CSPM consente di monitorare il livello di conformità e sicurezza in tutto l'ambiente. AWS

Riduzione dell'impegno per la raccolta e la definizione della priorità dei risultati

Security Hub CSPM riduce lo sforzo di raccogliere e assegnare priorità ai risultati di sicurezza tra gli account dei prodotti integrati Servizi AWS e dei partner. AWS Security Hub CSPM elabora la ricerca dei dati utilizzando il AWS Security Finding Format (ASFF), un formato di ricerca standard. Ciò elimina la necessità di gestire i risultati provenienti da una miriade di fonti in più formati. Security Hub CSPM mette inoltre in correlazione i risultati dei diversi provider per aiutarti a dare priorità a quelli più importanti.

Controlli di sicurezza automatici rispetto alle best practice e agli standard

Security Hub CSPM esegue automaticamente controlli continui di configurazione e sicurezza a livello di account in base alle AWS migliori pratiche e agli standard del settore. Security Hub

CSPM utilizza i risultati di questi controlli per calcolare i punteggi di sicurezza e identifica account e risorse specifici che richiedono attenzione.

Vista consolidata dei risultati per account e provider

Security Hub CSPM consolida i risultati di sicurezza su account e prodotti del provider e visualizza i risultati sulla console Security Hub CSPM. Puoi anche recuperare i risultati tramite l'API CSPM o gli SDK di Security Hub. AWS CLI Con una visione olistica dello stato di sicurezza attuale, puoi individuare tendenze, identificare potenziali problemi e adottare le misure correttive necessarie.

Capacità di automatizzare la ricerca di aggiornamenti e correzioni

È possibile creare regole di automazione che modificano o sopprimono i risultati in base ai criteri definiti. Security Hub CSPM supporta anche l'integrazione con Amazon. EventBridge Per automatizzare la correzione di risultati specifici, puoi definire azioni personalizzate da intraprendere quando viene generato un risultato. Ad esempio, puoi configurare operazioni personalizzate per inviare risultati a un sistema di ticket o a un sistema di correzione automatizzato.

Accesso a Security Hub CSPM

Security Hub CSPM è disponibile nella maggior parte dei casi. Regioni AWS Per un elenco delle regioni in cui Security Hub CSPM è attualmente disponibile, consulta Endpoint e quote CSPM di AWS Security Hub in. Riferimenti generali di AWS Per informazioni sulla gestione Regioni AWS del tuo account Account AWS, consulta Specificazione dell'account che il Regioni AWS tuo account può utilizzare nella Guida di riferimento.Gestione dell'account AWS

In ogni regione, puoi accedere e utilizzare Security Hub CSPM in uno dei seguenti modi:

Console CSPM Security Hub

Console di gestione AWS È un'interfaccia basata su browser che è possibile utilizzare per creare e gestire risorse. AWS Come parte di tale console, la console Security Hub CSPM fornisce l'accesso all'account, ai dati e alle risorse CSPM di Security Hub. È possibile eseguire attività CSPM di Security Hub utilizzando la console Security Hub CSPM: visualizzare i risultati, creare regole di automazione, creare un'area di aggregazione e altro ancora.

API CSPM DEL Security Hub

L'API CSPM di Security Hub ti offre l'accesso programmatico all'account, ai dati e alle risorse CSPM di Security Hub. Con l'API, puoi inviare richieste HTTPS direttamente a Security Hub CSPM. Per informazioni sull'API, consulta l'AWS Security Hub API Reference.

AWS CLI

Con AWS CLI, è possibile eseguire comandi dalla riga di comando del sistema per eseguire attività CSPM di Security Hub. In alcuni casi, l'utilizzo della riga di comando può essere più rapido e comodo rispetto all'utilizzo della console. La riga di comando è utile anche se si desidera creare script che eseguano operazioni. Per informazioni sull'installazione e l'utilizzo di AWS CLI, consultate la Guida per l'AWS Command Line Interface utente.

AWS SDK

AWS fornisce SDK costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione, ad esempio Java, Go, Python, C++ e.NET. Gli SDK forniscono un accesso pratico e programmatico a Security Hub CSPM e ad altri Servizi AWS nella lingua preferita. Gestiscono anche attività come la firma crittografica delle richieste, la gestione degli errori e il ritentativo automatico delle richieste. Per informazioni sull'installazione e l'utilizzo degli AWS SDK, consulta Tools to Build on. AWS

Important

Security Hub CSPM rileva e consolida solo i risultati generati dopo aver abilitato Security Hub CSPM. Non rileva e consolida retroattivamente i risultati di sicurezza generati prima dell'attivazione di Security Hub CSPM.
Security Hub CSPM riceve ed elabora i risultati solo nella regione in cui hai abilitato Security Hub CSPM nel tuo account.
Per la piena conformità ai controlli di sicurezza di CIS AWS Foundations Benchmark, è necessario abilitare Security Hub CSPM in tutte le regioni supportate. AWS

Servizi correlati

Per proteggere ulteriormente il tuo AWS ambiente, prendi in considerazione l'utilizzo di altri Servizi AWS in combinazione con Security Hub CSPM. Alcuni Servizi AWS inviano i risultati a Security

Hub CSPM e Security Hub CSPM normalizza i risultati in un formato standard. Alcuni Servizi AWS possono anche ricevere i risultati dal Security Hub CSPM.

Per un elenco delle altre persone Servizi AWS che inviano o ricevono risultati CSPM di Security Hub, vedere. Servizio AWS integrazioni con Security Hub CSPM

Security Hub CSPM utilizza regole collegate ai servizi AWS Config per eseguire i controlli di sicurezza per la maggior parte dei controlli. I controlli si riferiscono a risorse e specifiche. Servizi AWS AWS Per un elenco dei controlli CSPM di Security Hub, vedere. Riferimento di controllo per Security Hub CSPM È necessario abilitare AWS Config e registrare le risorse in Security Hub CSPM AWS Config per generare la maggior parte dei risultati di controllo. Per ulteriori informazioni, consulta Considerazioni prima dell'attivazione e della configurazione AWS Config.

Versione di prova gratuita e prezzi di Security Hub CSPM

Quando abiliti Security Hub CSPM Account AWS per la prima volta, quell'account viene automaticamente registrato a una prova gratuita di 30 giorni di Security Hub CSPM.

Quando utilizzi Security Hub CSPM durante la prova gratuita, ti viene addebitato l'utilizzo di altri servizi con cui interagisce Security Hub CSPM, come gli articoli. AWS Config Non ti vengono addebitati costi per AWS Config le regole attivate solo dagli standard di sicurezza CSPM di Security Hub.

Non ti verrà addebitato alcun costo per l'utilizzo del CSPM di Security Hub fino al termine della prova gratuita.

Visualizzazione dei dettagli di utilizzo

Security Hub CSPM fornisce informazioni sull'utilizzo, incluso il numero di controlli e risultati di sicurezza elaborati dal tuo account. I dettagli di utilizzo includono anche il tempo residuo della prova gratuita. Queste informazioni possono aiutarti a comprendere l'utilizzo del CSPM di Security Hub al termine del periodo di prova gratuito. Le informazioni sull'utilizzo sono disponibili anche al termine del periodo di prova gratuito.

Per visualizzare le informazioni sull'utilizzo (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Utilizzo in Impostazioni.

Le informazioni sull'utilizzo sono solo per l'account corrente e la regione corrente. In una regione di aggregazione, le informazioni sull'utilizzo non includono le regioni collegate. Per ulteriori informazioni sulle regioni collegate, consultathe section called "Tipi di dati aggregati".

Per visualizzare i dettagli dei costi del tuo account, utilizza la console di AWS fatturazione.

Dettagli prezzi

Per ulteriori informazioni su come Security Hub CSPM addebita i risultati acquisiti e i controlli di sicurezza, consulta i prezzi di Security Hub CSPM.

Concetti e terminologia in Security Hub CSPM

In AWS Security Hub CSPM, ci basiamo su AWS concetti e terminologia comuni e utilizziamo questi termini aggiuntivi.

Account

Un account Amazon Web Services (AWS) standard che contiene le tue risorse. AWS Puoi accedere AWS con il tuo account e abilitare Security Hub CSPM.

Un account può invitare altri account ad abilitare Security Hub CSPM e ad associarsi a quell'account in Security Hub CSPM. L'accettazione di un invito è facoltativa. Se gli inviti vengono accettati, l'account diventa un account amministratore e gli account aggiunti sono account membri. Gli account amministratore possono visualizzare i risultati nei rispettivi account membri.

Se sei iscritto AWS Organizations, l'organizzazione designa un account amministratore CSPM di Security Hub per l'organizzazione. L'account amministratore CSPM di Security Hub può abilitare altri account dell'organizzazione come account membri.

Un account non può essere contemporaneamente un account amministratore e un account membro. Un account può avere un solo account amministratore.

Per ulteriori informazioni, consulta Gestione degli account di amministratore e membro in Security Hub CSPM.

Account amministratore

Un account in Security Hub CSPM a cui è concesso l'accesso per visualizzare i risultati degli account membri associati.

Un account diventa un account amministratore in uno dei seguenti modi:

- L'account invita altri account ad associarsi ad esso in Security Hub CSPM. Quando tali account accettano l'invito, diventano account membri e l'account che invita diventa il loro account amministratore.
- L'account è designato da un account di gestione dell'organizzazione come account amministratore CSPM di Security Hub. L'account amministratore CSPM di Security Hub può abilitare qualsiasi account dell'organizzazione come account membro e può anche invitare altri account a diventare membri.

Un account può avere un solo account amministratore. Un account non può essere contemporaneamente un account amministratore e un account membro.

Regione di aggregazione

L'impostazione di una regione di aggregazione consente di visualizzare i risultati di sicurezza di più elementi Regioni AWS in un unico pannello di controllo.

La regione di aggregazione è la regione da cui è possibile visualizzare e gestire i risultati. I risultati vengono aggregati nella regione di aggregazione dalle regioni collegate. Gli aggiornamenti dei risultati vengono replicati in tutte le regioni.

Nella regione di aggregazione, le pagine degli standard di sicurezza, degli approfondimenti e dei risultati includono i dati di tutte le regioni collegate.

Per ulteriori informazioni, consulta the section called "Aggregazione dei dati tra le regioni".

Risultati archiviati

Un risultato il cui stato di registrazione (`RecordState`) è`ARCHIVED`. L'archiviazione di un risultato indica che il fornitore dei risultati ritiene che il risultato non sia più pertinente. Lo stato del record è diverso dallo stato del flusso di lavoro, che tiene traccia dello stato dell'indagine in un risultato.

I fornitori di servizi di ricerca possono utilizzare il BatchImportFindings funzionamento dell'API Security Hub CSPM per archiviare i risultati da loro creati. Security Hub CSPM archivia automaticamente i risultati di controllo che soddisfano determinati criteri. Per ulteriori informazioni, consulta Generazione, aggiornamento e archiviazione dei risultati di controllo.

Sulla console Security Hub CSPM, le impostazioni di filtro predefinite escludono i risultati archiviati dagli elenchi e dalle tabelle dei risultati. È possibile aggiornare le impostazioni per includere i risultati archiviati. Se si recuperano i risultati utilizzando l'GetFindingsAPI CSPM di Security Hub,

l'operazione recupera sia i risultati archiviati che quelli attivi. Per escludere i risultati archiviati, puoi filtrare i risultati. Ad esempio:

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
],
```

AWS Security Finding Format (ASFF)

Un formato standardizzato per il contenuto dei risultati che Security Hub CSPM aggrega o genera. Il AWS Security Finding Format consente di utilizzare Security Hub CSPM per visualizzare e analizzare i risultati generati dai servizi di sicurezza, dalle soluzioni di terze parti o dallo AWS stesso Security Hub CSPM durante l'esecuzione dei controlli di sicurezza. Per ulteriori informazioni, consulta AWS Formato ASFF (Security Finding Format).

Controllo

Una salvaguardia o contromisura prescritta per un sistema informatico o un'organizzazione concepita per proteggere la riservatezza, l'integrità e la disponibilità delle sue informazioni e per soddisfare una serie di requisiti di sicurezza definiti. Uno standard di sicurezza è associato a una raccolta di controlli.

Il termine controllo di sicurezza si riferisce ai controlli con un unico ID di controllo e titolo per tutti gli standard. Il termine controllo standard si riferisce ai controlli con ID di controllo e titoli specifici dello standard. Attualmente, Security Hub CSPM supporta i controlli standard solo nelle regioni della Cina e. AWS GovCloud (US) Regions I controlli di sicurezza sono supportati in tutte le altre regioni.

Operazione personalizzata

Un meccanismo CSPM di Security Hub per l'invio di risultati selezionati a. EventBridge Un'azione personalizzata viene creata in Security Hub CSPM. Viene quindi collegata a una EventBridge regola. La regola definisce un'operazione specifica da eseguire quando viene ricevuta una ricerca associata all'ID operazione personalizzato. Le operazioni personalizzate possono essere utilizzate, ad esempio, per inviare una ricerca specifica, o un piccolo set di risultati, a un flusso di lavoro di risposta o di correzione. Per ulteriori informazioni, consulta the section called “Creazione di un'azione personalizzata”.

Account amministratore delegato (organizzazioni)

In AWS Organizations, l'account amministratore delegato di un servizio è in grado di gestire l'uso di un servizio per l'organizzazione.

In Security Hub CSPM, l'account amministratore Security Hub CSPM è anche l'account amministratore delegato per Security Hub CSPM. Quando l'account di gestione dell'organizzazione designa per la prima volta un account amministratore di Security Hub CSPM, Security Hub CSPM chiama le organizzazioni per rendere quell'account l'account amministratore delegato.

L'account di gestione dell'organizzazione deve quindi scegliere l'account amministratore delegato come account amministratore CSPM di Security Hub in tutte le regioni.

Risultato

La registrazione osservabile di un controllo di sicurezza o di un rilevamento correlato alla sicurezza. Security Hub CSPM genera e aggiorna i risultati dopo aver completato i controlli di sicurezza per i controlli. Questi sono chiamati risultati di controllo. I risultati possono provenire anche da integrazioni con altri prodotti Servizi AWS e di terze parti.

Per ulteriori informazioni, consulta the section called "Esiti".

Cross-Region aggregazione

L'aggregazione di risultati, approfondimenti, stati di conformità di controllo e punteggi di sicurezza dalle regioni collegate a un'area di aggregazione. Puoi quindi visualizzare tutti i dati della regione di aggregazione e aggiornare i risultati e gli approfondimenti della regione di aggregazione.

Per ulteriori informazioni, consulta the section called "Aggregazione dei dati tra le regioni".

Individuazione dell'ingestione

L'importazione di risultati in Security Hub CSPM da altri AWS servizi e da fornitori partner terzi.

Gli eventi di Finding ingestion includono sia nuovi risultati che aggiornamenti ai risultati esistenti.

Informazione dettagliata

Una raccolta di risultati correlati definiti da un'istruzione di aggregazione e filtri opzionali. Un approfondimento identifica un'area di sicurezza che richiede attenzione e intervento. Security Hub CSPM offre diverse informazioni gestite (predefinite) che non è possibile modificare. Puoi anche creare approfondimenti CSPM di Security Hub personalizzati per tenere traccia dei problemi di

sicurezza specifici del tuo ambiente e del tuo AWS utilizzo. Per ulteriori informazioni, consulta the section called "Approfondimenti".

Regione collegata

Quando abiliti l'aggregazione interregionale, una regione collegata è un'area che aggrega risultati, approfondimenti, controlla gli stati di conformità e i punteggi di sicurezza nella regione di aggregazione.

In una regione collegata, le pagine Risultati e approfondimenti contengono i risultati solo di quella regione.

Per ulteriori informazioni, consulta the section called "Aggregazione dei dati tra le regioni".

Account membro

Un account che ha concesso a un account amministratore l'autorizzazione a visualizzare i risultati e ad agire in base a tali risultati.

Un account diventa un account membro in uno dei seguenti modi:

- L'account accetta un invito da un altro account.
- Per un account aziendale, l'account amministratore Security Hub CSPM abilita l'account come account membro.

Requisiti correlati

Un set di requisiti di settore o normativi mappati a un controllo.

Regola

Un set di criteri automatizzati utilizzati per valutare se un controllo viene rispettato. Quando viene valutata una regola, il risultato può essere positivo o negativo. Se la valutazione non è in grado di determinare se la regola ha esito negativo o positivo, la regola è in uno stato di avviso. Se la regola non può essere valutata, significa che è in uno stato non disponibile.

Controllo di sicurezza

Una valutazione puntuale specifica di una regola rispetto a una singola risorsa risultante in uno stato`PASSED`,, `FAILED` o. `WARNING` `NOT_AVAILABLE` L'esecuzione di un controllo di sicurezza produce un risultato.

Account amministratore CSPM di Security Hub

Un account dell'organizzazione che gestisce l'iscrizione al Security Hub CSPM per un'organizzazione.

L'account di gestione dell'organizzazione designa l'account amministratore CSPM di Security Hub in ciascuna regione. L'account di gestione dell'organizzazione deve scegliere lo stesso account amministratore CSPM di Security Hub in tutte le regioni.

L'account amministratore Security Hub CSPM è anche l'account amministratore delegato per Security Hub CSPM nelle organizzazioni.

L'account amministratore Security Hub CSPM può abilitare qualsiasi account dell'organizzazione come account membro. L'account amministratore CSPM di Security Hub può anche invitare altri account a diventare account membri.

Standard di sicurezza

Un'istruzione pubblicata su un argomento che specifica le caratteristiche, di solito misurabili e sotto forma di controlli, che devono essere soddisfatte o archiviate per conformità. Gli standard di sicurezza possono essere basati su framework normativi, best practice o policy aziendali interne. Un controllo può essere associato a uno o più standard supportati in Security Hub CSPM. Per ulteriori informazioni sugli standard di sicurezza in Security Hub CSPM, vedere. Comprensione degli standard di sicurezza in Security Hub CSPM

Gravità

La gravità assegnata a un controllo CSPM di Security Hub identifica l'importanza del controllo. La gravità di un controllo può essere critica, alta, media , bassa o informativa. La gravità assegnata ai risultati del controllo è uguale alla gravità del controllo stesso. Per informazioni su come Security Hub CSPM assegna la gravità a un controllo, consulta. Livelli di gravità per i risultati del controllo

Stato del flusso di lavoro

Lo stato di un'indagine su un risultato. Questo viene tracciato utilizzando l'attributo. `Workflow.Status`

Lo stato del flusso di lavoro è inizialmente `NEW`. Se hai notificato al proprietario della risorsa che viene intrapresa un'azione per il risultato, puoi impostare lo stato del flusso di lavoro su `NOTIFIED`. Se il risultato non è un problema e non richiede alcuna azione, imposta lo stato del flusso di lavoro su `SUPPRESSED`. Dopo aver esaminato e risolto un risultato, imposta lo stato del flusso di lavoro su `RESOLVED`.

Per impostazione predefinita, la maggior parte degli elenchi di risultati include solo risultati con stato del flusso di lavoro `NEW` o `NOTIFIED`. Gli elenchi di risultati per i controlli includono anche i risultati `RESOLVED`.

Per l'operazione GetFindings, puoi includere un filtro per lo stato del flusso di lavoro.

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

La console Security Hub CSPM offre un'opzione per impostare lo stato del flusso di lavoro per i risultati. I clienti (o gli strumenti SIEM, creazione di ticket, gestione degli incidenti o SOAR che lavorano per conto di un cliente per aggiornare i risultati dei provider di risultati) possono anche utilizzare BatchUpdateFindings per aggiornare lo stato del flusso di lavoro.

Abilitazione di Security Hub CSPM

Esistono due modi per abilitare AWS Security Hub CSPM, mediante l'integrazione o manualmente. AWS Organizations

Consigliamo vivamente l'integrazione con le organizzazioni per ambienti con più account e più regioni. Se disponi di un account autonomo, è necessario configurare Security Hub CSPM manualmente.

Verifica delle autorizzazioni necessarie

Dopo esserti registrato ad Amazon Web Services (AWS), devi abilitare Security Hub CSPM per utilizzarne le capacità e le caratteristiche. Per abilitare Security Hub CSPM, devi prima configurare le autorizzazioni che ti consentano di accedere alla console Security Hub CSPM e alle operazioni API. Tu o il tuo AWS amministratore potete farlo utilizzando AWS Identity and Access Management (IAM) per allegare la policy AWS gestita chiamata `AWSSecurityHubFullAccess` alla vostra identità IAM.

Per abilitare e gestire Security Hub CSPM tramite l'integrazione delle organizzazioni, è inoltre necessario allegare la policy AWS gestita denominata. `AWSSecurityHubOrganizationsAccess`

Per ulteriori informazioni, consulta AWS politiche gestite per Security Hub.

Abilitazione di Security Hub CSPM con l'integrazione delle organizzazioni

Per iniziare a utilizzare Security Hub CSPM con AWS Organizations, l'account di AWS Organizations gestione dell'organizzazione designa un account come account amministratore delegato di Security

Hub CSPM per l'organizzazione. Security Hub CSPM viene abilitato automaticamente nell'account amministratore delegato nella regione corrente.

Scegli il metodo preferito e segui i passaggi per designare l'amministratore delegato.

Security Hub CSPM console

Per designare l'amministratore CSPM delegato di Security Hub al momento dell'onboarding

1. Aprire la console CSPM di AWS Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Scegli Vai a Security Hub CSPM. Ti viene richiesto di accedere all'account di gestione dell'organizzazione.
3. Nella pagina Designazione dell'amministratore delegato, nella sezione Account amministratore delegato, specifica l'account amministratore delegato. Ti consigliamo di scegliere lo stesso amministratore delegato che hai impostato per altri AWS servizi di sicurezza e conformità.
4. Scegli Imposta amministratore delegato.

Security Hub CSPM API

Richiama l'`EnableOrganizationAdminAccount`API dall'account di gestione dell'organizzazione. Fornisci l' Account AWS ID dell'account amministratore delegato CSPM di Security Hub.

AWS CLI

Esegui il `enable-organization-admin-account` comando dall'account di gestione dell'organizzazione. Fornisci l' Account AWS ID dell'account amministratore delegato CSPM di Security Hub.

Esempio di comando:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Per ulteriori informazioni sull'integrazione con le organizzazioni, consultaIntegrazione del Security Hub CSPM conAWS Organizations.

Configurazione centrale

Quando integri Security Hub CSPM e Organizations, hai la possibilità di utilizzare una funzionalità chiamata configurazione centrale per configurare e gestire Security Hub CSPM per la tua organizzazione. Consigliamo vivamente di utilizzare la configurazione centrale perché consente all'amministratore di personalizzare la copertura di sicurezza per l'organizzazione. Ove appropriato, l'amministratore delegato può consentire a un account membro di configurare le proprie impostazioni di copertura di sicurezza.

La configurazione centrale consente all'amministratore delegato di configurare Security Hub CSPM su più account, unità organizzative e. Regioni AWS L'amministratore delegato configura Security Hub CSPM creando policy di configurazione. All'interno di una politica di configurazione, è possibile specificare le seguenti impostazioni:

- Se Security Hub CSPM è abilitato o disabilitato
- Quali standard di sicurezza sono abilitati e disattivati
- Quali controlli di sicurezza sono abilitati e disattivati
- Se personalizzare i parametri per determinati controlli

In qualità di amministratore delegato, puoi creare un'unica politica di configurazione per l'intera organizzazione o politiche di configurazione diverse per i vari account e unità organizzative. Ad esempio, gli account di test e gli account di produzione possono utilizzare politiche di configurazione diverse.

Gli account dei membri e le unità organizzative che utilizzano una politica di configurazione sono gestiti centralmente e possono essere configurati solo dall'amministratore delegato. L'amministratore delegato può designare account e unità organizzative specifici come autogestiti per dare al membro la possibilità di configurare le proprie impostazioni su base individuale. Region-by-Region

Se non si utilizza la configurazione centrale, è necessario in gran parte configurare Security Hub CSPM separatamente in ogni account e regione. Questa è chiamata configurazione locale. In base alla configurazione locale, l'amministratore delegato può abilitare automaticamente Security Hub CSPM e un set limitato di standard di sicurezza nei nuovi account dell'organizzazione nella regione corrente. La configurazione locale non si applica agli account dell'organizzazione esistenti o alle regioni diverse dalla regione corrente. La configurazione locale inoltre non supporta l'uso di politiche di configurazione.

Abilitazione manuale di Security Hub CSPM

È necessario abilitare Security Hub CSPM manualmente se si dispone di un account autonomo o se non si effettua l'integrazione con. AWS Organizations Gli account autonomi non possono integrarsi AWS Organizations e devono utilizzare l'abilitazione manuale.

Quando si abilita Security Hub CSPM manualmente, si designa un account amministratore di Security Hub CSPM e si invitano altri account a diventare account membri. La relazione amministratore-membro viene stabilita quando un potenziale account membro accetta l'invito.

Scegli il tuo metodo preferito e segui i passaggi per abilitare Security Hub CSPM. Quando abiliti Security Hub CSPM dalla console, hai anche la possibilità di abilitare gli standard di sicurezza supportati.

Security Hub CSPM console

1. Aprire la console AWS Security Hub CSPM all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Quando apri la console Security Hub CSPM per la prima volta, scegli Vai a Security Hub CSPM.
3. Nella pagina di benvenuto, la sezione Standard di sicurezza elenca gli standard di sicurezza supportati da Security Hub CSPM.

   Seleziona la casella di controllo relativa a uno standard per abilitarlo e deseleziona la casella di controllo per disabilitarlo.

   È possibile abilitare o disabilitare uno standard o i relativi controlli singoli in qualsiasi momento. Per informazioni sulla gestione degli standard di sicurezza, vedereComprensione degli standard di sicurezza in Security Hub CSPM.
4. Scegliere Enable Security Hub (Abilita Security Hub).

Security Hub CSPM API

Richiama l'`EnableSecurityHub`API. Quando si abilita Security Hub CSPM dall'API, vengono abilitati automaticamente i seguenti standard di sicurezza predefiniti:

- AWS Best practice fondamentali per la sicurezza
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

Se non desideri abilitare questi standard, imposta `EnableDefaultStandards` su `false`.

È inoltre possibile utilizzare il `Tags` parametro per assegnare valori di tag alla risorsa hub.

AWS CLI

Esegui il comando `enable-security-hub`. Per abilitare gli standard predefiniti, includi`--enable-default-standards`. Per non abilitare gli standard predefiniti, includi`--no-enable-default-standards`. Gli standard di sicurezza predefiniti sono i seguenti:

- AWS Best practice fondamentali in materia di sicurezza
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

Esempio

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

Multi-account script di abilitazione

> **Note**
>
> Invece di questo script, consigliamo di utilizzare la configurazione centrale per abilitare e configurare Security Hub CSPM su più account e regioni.

Lo script di abilitazione multi-account Security Hub CSPM in GitHub consente di abilitare Security Hub CSPM tra account e regioni. Lo script automatizza inoltre il processo di invio e attivazione degli inviti agli account dei membri. AWS Config

Lo script abilita automaticamente la registrazione AWS Config delle risorse per tutte le risorse, comprese le risorse globali, in tutte le regioni. Non limita la registrazione delle risorse globali a una singola regione. Per ridurre i costi, consigliamo di registrare le risorse globali in una sola regione. Se utilizzi la configurazione centrale o l'aggregazione interregionale, questa dovrebbe essere la tua regione di origine. Per ulteriori informazioni, consulta Registrazione delle risorse in AWS Config.

È disponibile uno script corrispondente per disabilitare Security Hub CSPM tra account e regioni.

Passaggi successivi: gestione e integrazioni della postura

Dopo aver abilitato Security Hub CSPM, ti consigliamo di abilitare gli standard e i controlli di sicurezza per monitorare il tuo stato di sicurezza. Dopo aver abilitato i controlli, Security Hub CSPM inizia a eseguire i controlli di sicurezza e a generare risultati di controllo che consentono di rilevare configurazioni errate nell'ambiente. AWS Per ricevere i risultati del controllo, è necessario abilitare e configurare AWS Config Security Hub CSPM. Per ulteriori informazioni, consulta Attivazione e configurazione AWS Config per Security Hub CSPM.

Dopo aver abilitato Security Hub CSPM, puoi anche sfruttare le integrazioni tra Security Hub CSPM Servizi AWS e altre soluzioni di terze parti per visualizzarne i risultati in Security Hub CSPM. Security Hub CSPM aggrega i risultati provenienti da diverse fonti e li inserisce in un formato coerente. Per ulteriori informazioni, consulta Comprendere le integrazioni in Security Hub CSPM.

Attivazione e configurazione AWS Config per Security Hub CSPM

AWS Security Hub CSPM utilizza AWS Config regole per eseguire controlli di sicurezza e generare risultati per la maggior parte dei controlli. AWS Config fornisce una visualizzazione dettagliata della configurazione delle AWS risorse del tuo. Account AWS Utilizza regole per stabilire una configurazione di base per le risorse e un registratore di configurazione per rilevare se una particolare risorsa viola le condizioni di una regola.

Alcune regole, denominate regole AWS Config gestite, sono predefinite e sviluppate da. AWS Config Altre regole sono AWS Config regole personalizzate sviluppate da Security Hub CSPM. AWS Config le regole utilizzate da Security Hub CSPM per i controlli sono denominate regole collegate ai servizi. Service-linked regole Servizi AWS come Security Hub CSPM consentono di creare AWS Config regole nel tuo account.

Se hai abilitato sia AWS Security Hub CSPM che Security Hub, Security Hub CSPM crea automaticamente un registratore di configurazione collegato al servizio per valutare i controlli di sicurezza. Non è necessario abilitare o configurare manualmente. AWS Config Per ulteriori informazioni, consulta Utilizzo del registratore di configurazione collegato al servizio.

Se Security Hub CSPM è abilitato senza Security Hub, è necessario abilitare AWS Config e attivare manualmente la registrazione delle risorse. Per ulteriori informazioni, consulta Configurazione manuale AWS Config.

I AWS Config prerequisiti descritti in questa pagina si applicano solo agli standard di sicurezza, come AWS Foundational AWS Security Best Practices e AWS CIS Foundations Benchmark. Gli standard multicloud, come CIS Azure Foundations Benchmark v4.0.0, non richiedono l'abilitazione della registrazione o la configurazione di un registratore di configurazione. AWS Config Il connettore multicloud Security Hub CSPM configura automaticamente un registratore collegato al servizio per valutare le risorse cloud esterne. L'unico prerequisito per gli standard multicloud è un connettore CSPM Security Hub per il provider cloud esterno.

Argomenti

- Utilizzo del registratore di configurazione collegato al servizio
- Configurazione manuale AWS Config
- Comprendere il controllo Config.1
- Generazione di regole legate ai servizi

Utilizzo del registratore di configurazione collegato al servizio

Quando hai abilitato sia AWS Security Hub CSPM che Security Hub, Security Hub CSPM crea e gestisce automaticamente un registratore di configurazione collegato al servizio tra i tuoi account e le tue regioni. Non è necessario abilitare o configurare manualmente. AWS Config

Il nome di questo registratore di configurazione è`AWSConfigurationRecorderForSecurityHubCSPM`. Security Hub CSPM crea un registratore di configurazione collegato al servizio corrispondente per ogni account e regione in cui sono abilitati sia Security Hub CSPM che Security Hub. Quando abiliti Security Hub CSPM per Account AWS i nuovi messaggi, Security Hub CSPM crea automaticamente il registratore di configurazione collegato al servizio. Regione AWS

Security Hub CSPM gestisce la configurazione delle risorse del registratore di configurazione collegato al servizio, garantendo che la registrazione sia abilitata per tutte le risorse legate ai controlli supportati da Security Hub. Per un elenco delle risorse necessarie, vedere. Richiesto AWS Config risorse per i risultati del controllo

Quando Security Hub CSPM crea questo registratore di configurazione collegato al servizio, Security Hub non utilizza il registratore di configurazione gestito dal cliente in. AWS Config

Per ulteriori informazioni sui registratori di configurazione, consulta Lavorare con il registratore di configurazione nella Guida per gli sviluppatori.AWS Config

Configurazione manuale AWS Config

I seguenti passaggi si applicano quando Security Hub CSPM è abilitato senza Security Hub. In questo caso, è necessario abilitare AWS Config l'account e attivare la registrazione delle risorse per i tipi di risorse valutati dai controlli abilitati. Dopo aver eseguito questa operazione, Security Hub CSPM crea le AWS Config regole appropriate e inizia a eseguire i controlli di sicurezza per generare i risultati.

Considerazioni prima dell'attivazione e della configurazione AWS Config

Per ricevere i risultati del controllo in Security Hub CSPM, AWS Config devi abilitarli per il tuo account in tutti i paesi in Regione AWS cui è abilitato Security Hub CSPM. Se si utilizza Security Hub CSPM per un ambiente con più account, AWS Config deve essere abilitato in ogni regione per l'account amministratore e tutti gli account dei membri.

Ti consigliamo vivamente di attivare la registrazione delle risorse AWS Config prima di abilitare qualsiasi standard e controllo CSPM di Security Hub. Questo ti aiuta a garantire che i risultati dei controlli siano accurati.

Per attivare la registrazione delle risorse AWS Config, devi disporre di autorizzazioni sufficienti per registrare le risorse nel ruolo AWS Identity and Access Management (IAM) collegato al registratore di configurazione. Inoltre, assicurati che nessuna policy o AWS Organizations policy IAM AWS Config impedisca di avere l'autorizzazione a registrare le tue risorse. I controlli CSPM di Security Hub valutano direttamente le configurazioni delle risorse e non tengono conto delle AWS Organizations politiche. Per ulteriori informazioni sulla AWS Config registrazione, consulta Lavorare con il registratore di configurazione nella Guida per gli sviluppatori.AWS Config

Se abiliti uno standard in Security Hub CSPM ma non lo hai abilitato AWS Config, Security Hub CSPM tenta di creare AWS Config regole collegate ai servizi secondo la seguente pianificazione:

- Il giorno in cui abiliti lo standard.
- Il giorno dopo aver abilitato lo standard.
- 3 giorni dopo l'attivazione dello standard.
- 7 giorni dopo l'attivazione dello standard e successivamente in modo continuativo ogni 7 giorni.

Se si utilizza la configurazione centrale, Security Hub CSPM tenta anche di creare AWS Config regole collegate ai servizi ogni volta che si associa una politica di configurazione che abilita uno o più standard agli account, alle unità organizzative (OU) o alla radice.

Registrazione delle risorse in AWS Config

Quando si abilita AWS Config, è necessario specificare quali AWS risorse si desidera che il registratore di AWS Config configurazione registri. Tramite le regole collegate al servizio, il registratore di configurazione consente a Security Hub CSPM di rilevare le modifiche alle configurazioni delle risorse.

Affinché Security Hub CSPM generi risultati di controllo accurati, è necessario attivare la registrazione AWS Config per i tipi di risorse che corrispondono ai controlli abilitati. Sono principalmente abilitati i controlli con un tipo di pianificazione innescato dalla modifica che richiedono la registrazione delle risorse. Alcuni controlli con un tipo di pianificazione periodica richiedono anche la registrazione delle risorse. Per un elenco di questi controlli e delle risorse corrispondenti, vedereRichiesto AWS Config risorse per i risultati del controllo.

> **Warning**
>
> Se non configuri correttamente AWS Config la registrazione per i controlli CSPM di Security Hub, i risultati dei controlli possono essere imprecisi, in particolare nei seguenti casi:
>
> - Non hai mai registrato la risorsa per un determinato controllo o hai disabilitato la registrazione di una risorsa prima di creare quel tipo di risorsa. In questi casi, riceverete un `WARNING` risultato relativo al controllo in questione, anche se potreste aver creato delle risorse nell'ambito del controllo dopo aver disattivato la registrazione. Questo `WARNING` risultato è un risultato predefinito che in realtà non valuta lo stato di configurazione della risorsa.
> - Si disabilita la registrazione per una risorsa che viene valutata da un particolare controllo. In questo caso, Security Hub CSPM conserva i risultati del controllo generati prima della disattivazione della registrazione, anche se il controllo non valuta risorse nuove o aggiornate. Security Hub CSPM modifica anche lo stato di conformità dei risultati in. `WARNING` Questi risultati conservati potrebbero non riflettere accuratamente lo stato di configurazione corrente di una risorsa.

Per impostazione predefinita, AWS Config registra tutte le risorse regionali supportate che rileva nell'ambiente Regione AWS in cui è in esecuzione. Per ricevere tutti i risultati del controllo CSPM di Security Hub, è inoltre necessario AWS Config configurare la registrazione delle risorse globali. Per risparmiare sui costi, consigliamo di registrare le risorse globali solo in una singola regione. Se utilizzi

la configurazione centrale o l'aggregazione tra regioni, questa regione dovrebbe essere la tua regione di origine.

In AWS Config, puoi scegliere tra la registrazione continua e la registrazione giornaliera delle modifiche allo stato delle risorse. Se si sceglie la registrazione giornaliera, AWS Config fornisce i dati di configurazione delle risorse alla fine di ogni periodo di 24 ore in caso di cambiamenti nello stato delle risorse. Se non ci sono modifiche, non viene fornito alcun dato. Ciò può ritardare la generazione dei risultati CSPM di Security Hub per i controlli attivati dalle modifiche fino al completamento di un periodo di 24 ore.

Per ulteriori informazioni sulla AWS Config registrazione, consulta Recording resources nella Developer Guide. AWS AWS Config

Modi per abilitare e configurare AWS Config

È possibile abilitare AWS Config e attivare la registrazione delle risorse in uno dei seguenti modi:

- AWS Config console: è possibile attivare AWS Config un account utilizzando la AWS Config console. Per istruzioni, consulta Configurazione AWS Config con la console nella Guida per gli AWS Config sviluppatori.
- AWS CLI o SDK: puoi abilitare AWS Config un account utilizzando AWS Command Line Interface (AWS CLI). Per istruzioni, consulta Configurazione AWS Config con AWS CLI nella Guida per gli AWS Config sviluppatori. AWS sono disponibili anche kit di sviluppo software (SDK) per molti linguaggi di programmazione.
- CloudFormation modello: AWS Config per abilitare più account, consigliamo di utilizzare il AWS CloudFormation modello denominato Enable. AWS Config Per accedere a questo modello, consulta i modelli di AWS CloudFormation StackSet esempio nella Guida AWS CloudFormation per l'utente.

  Per impostazione predefinita, questo modello esclude la registrazione per le risorse globali IAM. Assicurati di attivare la registrazione per le risorse globali IAM in una sola volta Regione AWS per ridurre i costi di registrazione. Se hai abilitato l'aggregazione tra regioni, questa dovrebbe essere la tua area di origine del Security Hub CSPM. Altrimenti, può essere qualsiasi regione in cui è disponibile Security Hub CSPM che supporta la registrazione di risorse globali IAM. Ti consigliamo di eseguirne una StackSet per registrare tutte le risorse, incluse le risorse globali IAM, nella regione principale o in un'altra regione selezionata. Quindi, esegui un secondo StackSet per registrare tutte le risorse tranne le risorse globali IAM in altre regioni.

- GitHub script — Security Hub CSPM offre uno GitHubscript che abilita Security Hub CSPM e AWS Config per più account tra le regioni. Questo script è utile se non hai ancora effettuato l'integrazione o se disponi AWS Organizations di alcuni account membri che non fanno parte di un'organizzazione.

Per ulteriori informazioni, consulta il seguente post sul blog sulla AWS sicurezza: Optimize AWS Config for AWS Security Hub CSPM per gestire efficacemente la tua posizione di sicurezza sul cloud.

Considerazioni sui costi

Security Hub CSPM può influire sui costi del registratore di AWS Config configurazione aggiornando l'`AWS::Config::ResourceCompliance`elemento di configurazione. Gli aggiornamenti possono avvenire ogni volta che un controllo CSPM di Security Hub associato a una AWS Config regola modifica lo stato di conformità, viene abilitato o disabilitato o presenta aggiornamenti dei parametri. Se utilizzi il registratore di AWS Config configurazione solo per Security Hub CSPM e non usi questo elemento di configurazione per altri scopi, ti consigliamo di disattivarne la registrazione. AWS Config Questo può ridurre i costi. AWS Config Non è necessario registrare i controlli di sicurezza `AWS::Config::ResourceCompliance` per funzionare in Security Hub CSPM.

Per informazioni sui costi associati alla registrazione delle risorse, consulta i prezzi e AWS Config i prezzi AWS di Security Hub CSPM.

Comprendere il controllo Config.1

> **Note**
>
> Quando AWS Security Hub CSPM e Security Hub sono entrambi abilitati, il Config.1 controllo ha sempre lo stato di. `PASSED` Security Hub CSPM ha accesso diretto agli elementi di configurazione tramite un registratore di configurazione collegato al servizio. Per ulteriori informazioni, consulta Utilizzo del registratore di configurazione collegato al servizio.

In Security Hub CSPM, il Config.1controllo genera `FAILED` risultati nel tuo account se AWS Config è disabilitato. Inoltre, genera `FAILED` risultati nel tuo account se AWS Config è abilitato ma la registrazione delle risorse non è attivata.

Se AWS Config è abilitata e la registrazione delle risorse è attivata, ma la registrazione delle risorse non è attivata per un tipo di risorsa controllata da un controllo abilitato, Security Hub CSPM genera

un `FAILED` risultato per il Config.1 controllo. Oltre a questo `FAILED` risultato, Security Hub CSPM genera `WARNING` risultati per il controllo abilitato e i tipi di risorse controllate dal controllo. Ad esempio, se si abilita il KMS.5controllo e la registrazione delle risorse non è attivata AWS KMS keys, Security Hub CSPM genera un `FAILED` risultato per il Config.1 controllo. Security Hub CSPM genera anche `WARNING` risultati per il KMS.5 controllo e le chiavi KMS.

Per ricevere un `PASSED` risultato relativo al Config.1 controllo, attiva la registrazione delle risorse per tutti i tipi di risorse che corrispondono ai controlli abilitati. Disattiva anche i controlli non necessari per la tua organizzazione. Questo aiuta a garantire che non vi siano lacune di configurazione nei controlli di sicurezza. Contribuisce inoltre a garantire la ricezione di risultati accurati sulle risorse configurate in modo errato.

Se sei l'amministratore CSPM delegato di Security Hub per un'organizzazione, la AWS Config registrazione deve essere configurata correttamente per il tuo account e i tuoi account membro. Se utilizzi l'aggregazione tra regioni, la AWS Config registrazione deve essere configurata correttamente nella regione d'origine e in tutte le regioni collegate. Non è necessario registrare le risorse globali nelle regioni collegate.

Generazione di regole legate ai servizi

Per ogni controllo che utilizza una AWS Config regola collegata al servizio, Security Hub CSPM crea istanze della regola richiesta nell'ambiente. AWS

Queste regole collegate ai servizi sono specifiche per Security Hub CSPM. Security Hub CSPM crea queste regole collegate ai servizi anche se esistono già altre istanze delle stesse regole. La regola collegata al servizio viene aggiunta `securityhub` prima del nome della regola originale e un identificatore univoco dopo il nome della regola. Ad esempio, per la regola AWS Config gestita`vpc-flow-logs-enabled`, il nome della regola collegata al servizio potrebbe essere. `securityhub-vpc-flow-logs-enabled-12345`

Esistono quote per il numero di regole AWS Config gestite che possono essere utilizzate per valutare i controlli. AWS Config le regole create da Security Hub CSPM non vengono conteggiate ai fini di tali quote. Puoi abilitare uno standard di sicurezza anche se hai già raggiunto la AWS Config quota di regole gestite nel tuo account. Per ulteriori informazioni sulle quote per AWS Config le regole, consulta la sezione Limiti del servizio AWS Config nella Guida per gli AWS Config sviluppatori.

> **Note**
>
> Se utilizzi Security Hub CSPM e Security Hub, puoi vedere le regole collegate ai servizi AWS Config ma non potrai vedere le risorse conformi o non conformi associate alla regola. Le risorse conformi e non conformi saranno visibili solo in Security Hub CSPM e Security Hub.

Comprendere la configurazione locale in Security Hub CSPM

La configurazione locale è il modo predefinito in cui un'AWSorganizzazione viene configurata in Security Hub CSPM. Se non si attiva e non si abilita la configurazione centrale, l'organizzazione utilizza la configurazione locale per impostazione predefinita.

Nella configurazione locale, l'account amministratore CSPM di Security Hub delegato ha un controllo limitato sulle impostazioni di configurazione. Le uniche impostazioni che l'amministratore delegato può applicare sono l'abilitazione automatica del Security Hub CSPM e degli standard di sicurezza predefiniti nei nuovi account dell'organizzazione. Queste impostazioni si applicano solo nella regione in cui è stato designato l'account amministratore delegato. Gli standard di sicurezza predefiniti sono AWS Foundational Security Best Practices (FSBP) e Center for Internet Security (CIS) Foundations Benchmark v1.2.0. AWS Le impostazioni di configurazione locali non si applicano agli account dell'organizzazione esistenti o alle regioni diverse da quella in cui è stato designato l'account amministratore delegato.

Oltre ad abilitare Security Hub CSPM e gli standard predefiniti nei nuovi account dell'organizzazione in una singola regione, è necessario configurare altre impostazioni CSPM di Security Hub, inclusi standard e controlli, separatamente in ogni regione e account. Poiché questo può essere un processo duplicato, consigliamo di utilizzare la configurazione centrale per un ambiente con più account se si verifica una o più delle seguenti condizioni:

- Desideri impostazioni di configurazione diverse per varie parti dell'organizzazione (ad esempio, standard o controlli abilitati diversi per team diversi).
- Operate in più regioni e desiderate ridurre i tempi e la complessità della configurazione del servizio in queste regioni.
- Desideri che i nuovi account utilizzino impostazioni di configurazione specifiche quando entrano a far parte dell'organizzazione.
- Vuoi che gli account dell'organizzazione ereditino impostazioni di configurazione specifiche da un account principale o root.

Per informazioni sulla configurazione centrale, vedereComprendere la configurazione centrale in Security Hub CSPM.

Comprendere la configurazione centrale in Security Hub CSPM

La configurazione centrale è una funzionalità CSPM di AWS Security Hub che consente di configurare e gestire Security Hub CSPM su più e. Account AWS Regioni AWS Per utilizzare la configurazione centrale, è necessario prima integrare Security Hub CSPM e. AWS OrganizationsÈ possibile integrare i servizi creando un'organizzazione e designando un account amministratore CSPM Security Hub delegato per l'organizzazione.

Dall'account amministratore CSPM di Security Hub delegato, puoi abilitare Security Hub CSPM per gli account e le unità organizzative (OU) della tua organizzazione in tutte le regioni. È inoltre possibile abilitare, configurare e disabilitare singoli standard di sicurezza e controlli di sicurezza per account e unità organizzative in tutte le regioni. È possibile configurare queste impostazioni in pochi passaggi da una regione principale, denominata regione di origine.

Quando si utilizza la configurazione centrale, l'amministratore delegato può scegliere quali account e unità organizzative configurare. Se l'amministratore delegato designa un account membro o un'unità organizzativa come autogestita, il membro può configurare le proprie impostazioni separatamente in ciascuna regione. Se l'amministratore delegato designa un account membro o un'unità organizzativa come gestita centralmente, solo l'amministratore delegato può configurare l'account membro o l'unità organizzativa in tutte le regioni. È possibile designare tutti gli account e le unità organizzative dell'organizzazione come gestiti centralmente, tutti autogestiti o una combinazione di entrambi.

Per configurare gli account gestiti centralmente, l'amministratore delegato utilizza le politiche di configurazione CSPM di Security Hub. Le politiche di configurazione consentono all'amministratore delegato di specificare se Security Hub CSPM è abilitato o disabilitato e quali standard e controlli sono abilitati o disabilitati. Possono essere utilizzati anche per personalizzare i parametri per determinati controlli.

Le politiche di configurazione hanno effetto nella regione di origine e in tutte le regioni collegate. L'amministratore delegato specifica la regione di origine dell'organizzazione e le regioni collegate prima di iniziare a utilizzare la configurazione centrale. La specificazione delle regioni collegate è facoltativa. L'amministratore delegato può creare un'unica politica di configurazione per l'intera organizzazione o creare più politiche di configurazione per configurare impostazioni variabili per account e unità organizzative diversi.

> **Tip**
>
> Se non si utilizza la configurazione centrale, è necessario configurare principalmente Security Hub CSPM separatamente in ogni account e regione. Questa è chiamata configurazione locale. Nella configurazione locale, l'amministratore delegato può abilitare automaticamente Security Hub CSPM e un set limitato di standard di sicurezza nei nuovi account dell'organizzazione nella regione corrente. La configurazione locale non si applica agli account dell'organizzazione esistenti o alle regioni diverse dalla regione corrente. Inoltre, la configurazione locale non supporta l'uso di politiche di configurazione.

Questa sezione fornisce una panoramica della configurazione centrale.

Vantaggi dell'utilizzo della configurazione centrale

I vantaggi della configurazione centrale includono quanto segue:

Semplifica la configurazione del servizio e delle funzionalità CSPM di Security Hub

Quando utilizzi la configurazione centrale, Security Hub CSPM ti guida attraverso il processo di configurazione delle best practice di sicurezza per la tua organizzazione. Inoltre, distribuisce automaticamente le politiche di configurazione risultanti su account e unità organizzative specifici. Se disponi di impostazioni CSPM di Security Hub esistenti, come l'abilitazione automatica di nuovi controlli di sicurezza, puoi utilizzarle come punto di partenza per le tue politiche di configurazione. Inoltre, la pagina di configurazione sulla console CSPM di Security Hub mostra un riepilogo in tempo reale delle policy di configurazione e degli account e delle unità organizzative che utilizzano ciascuna policy.

Configurazione su più account e regioni

È possibile utilizzare la configurazione centrale per configurare Security Hub CSPM su più account e regioni. Questo aiuta a garantire che ogni parte dell'organizzazione mantenga una configurazione coerente e una copertura di sicurezza adeguata.

Adatta configurazioni diverse in account e unità organizzative diversi

Con la configurazione centralizzata, puoi scegliere di configurare gli account e le unità organizzative della tua organizzazione in diversi modi. Ad esempio, gli account di test e gli account di produzione potrebbero richiedere configurazioni diverse. Puoi anche creare una politica di configurazione che copra i nuovi account quando entrano a far parte dell'organizzazione.

Previeni la deriva della configurazione

La modifica della configurazione si verifica quando un utente apporta una modifica a un servizio o a una funzionalità che è in conflitto con le selezioni dell'amministratore delegato. La configurazione centrale impedisce questa deriva. Quando si designa un account o un'unità organizzativa come gestito centralmente, tale account o unità organizzativa è configurabile solo dall'amministratore delegato dell'organizzazione. Se si preferisce che un account o un'unità organizzativa specifici configurino le proprie impostazioni, è possibile designarlo come autogestito.

Quando utilizzare la configurazione centrale?

La configurazione centrale è particolarmente utile per AWS gli ambienti che includono più account CSPM di Security Hub. È progettato per aiutarti a gestire centralmente Security Hub CSPM per più account.

È possibile utilizzare la configurazione centrale per configurare il servizio CSPM Security Hub, gli standard di sicurezza e i controlli di sicurezza. È inoltre possibile utilizzarlo per personalizzare i parametri di determinati controlli. Per ulteriori informazioni sugli standard di sicurezza, vedereComprensione degli standard di sicurezza in Security Hub CSPM. Per ulteriori informazioni sui controlli di sicurezza, vedereComprendere i controlli di sicurezza in Security Hub CSPM.

Termini e concetti relativi alla configurazione centrale

La comprensione dei seguenti termini e concetti chiave può aiutarti a utilizzare la configurazione centrale CSPM di Security Hub.

Configurazione centrale

Una funzionalità CSPM di Security Hub che aiuta l'account amministratore CSPM di Security Hub delegato per un'organizzazione a configurare il servizio CSPM Security Hub, gli standard di sicurezza e i controlli di sicurezza su più account e regioni. Per configurare queste impostazioni, l'amministratore delegato crea e gestisce le politiche di configurazione CSPM di Security Hub per gli account gestiti centralmente nella propria organizzazione. Self-managed gli account possono configurare le proprie impostazioni separatamente in ciascuna regione. Per utilizzare la configurazione centrale, è necessario integrare Security Hub CSPM e. AWS Organizations

Regione d'origine

Regione AWS Da cui l'amministratore delegato configura centralmente Security Hub CSPM, creando e gestendo le politiche di configurazione. Le politiche di configurazione hanno effetto nella regione di origine e in tutte le regioni collegate.

La regione di origine funge anche da regione di aggregazione CSPM del Security Hub e riceve risultati, approfondimenti e altri dati dalle regioni collegate.

Le regioni AWS introdotte a partire dal 20 marzo 2019 sono note come regioni opt-in. Una regione opt-in non può essere la regione di origine, ma può essere una regione collegata. Per un elenco delle regioni che hanno aderito, consulta Considerazioni prima di abilitare e disabilitare le regioni nella Guida di riferimento per la gestione degli AWS account.

Regione collegata

E Regione AWS che è configurabile dalla regione di origine. Le politiche di configurazione vengono create dall'amministratore delegato nella regione di origine. Le politiche hanno effetto nella regione di origine e in tutte le regioni collegate. La specificazione delle regioni collegate è facoltativa.

Una regione collegata invia inoltre risultati, approfondimenti e altri dati alla regione di origine.

Le regioni AWS introdotte a partire dal 20 marzo 2019 sono note come regioni opt-in. È necessario abilitare tale regione per un account prima di potervi applicare una politica di configurazione. L'account di gestione Organizations può abilitare le regioni opzionali per un account membro. Per ulteriori informazioni, consulta Specificare quali Regioni AWS account può essere utilizzato dal proprio account nella Guida di riferimento per la gestione degli AWS account.

Target

Un' Account AWS unità organizzativa (OU) o la radice dell'organizzazione.

Politica di configurazione CSPM di Security Hub

Una raccolta di impostazioni CSPM di Security Hub che l'amministratore delegato può configurare per destinazioni gestite centralmente. Questo include:

- Se abilitare o disabilitare Security Hub CSPM.
- Se abilitare uno o più standard di sicurezza.
- Quali controlli di sicurezza abilitare tra gli standard abilitati. L'amministratore delegato può farlo fornendo un elenco di controlli specifici che devono essere abilitati e Security Hub

CSPM disabilita tutti gli altri controlli (inclusi i nuovi controlli quando vengono rilasciati). In alternativa, l'amministratore delegato può fornire un elenco di controlli specifici che devono essere disabilitati e Security Hub CSPM abilita tutti gli altri controlli (inclusi i nuovi controlli quando vengono rilasciati).

- Facoltativamente, personalizza i parametri per selezionare i controlli abilitati tra gli standard abilitati.

Una politica di configurazione ha effetto nella regione di origine e in tutte le regioni collegate dopo essere stata associata ad almeno un account, un'unità organizzativa (OU) o la directory principale.

Sulla console Security Hub CSPM, l'amministratore delegato può scegliere la politica di configurazione consigliata da Security Hub CSPM o creare politiche di configurazione personalizzate. Con l'API Security Hub CSPM e AWS CLI, l'amministratore delegato può creare solo politiche di configurazione personalizzate. L'amministratore delegato può creare un massimo di 20 politiche di configurazione personalizzate.

Nella politica di configurazione consigliata, Security Hub CSPM, lo standard AWS Foundational Security Best Practices (FSBP) e tutti i controlli FSBP esistenti e nuovi sono abilitati. I controlli che accettano i parametri utilizzano i valori predefiniti. La politica di configurazione consigliata si applica all'intera organizzazione.

Per applicare impostazioni diverse all'organizzazione o applicare politiche di configurazione diverse a account e unità organizzative diversi, crea una politica di configurazione personalizzata.

> **Note**
>
> Le policy di configurazione supportano solo gli standard e i controlli di AWS sicurezza. Gli standard multicloud, come CIS Azure Foundations Benchmark v4.0.0, e i relativi controlli multicloud associati non possono essere inclusi in una politica di configurazione. Per abilitare o configurare gli standard multicloud, usa i meccanismi di configurazione locali direttamente nel file desiderato. Account AWS

Configurazione locale

Il tipo di configurazione predefinito per un'organizzazione, dopo l'integrazione di Security Hub CSPM e. AWS Organizations Con la configurazione locale, l'amministratore delegato può scegliere di abilitare automaticamente Security Hub CSPM e gli standard di sicurezza

predefiniti nei nuovi account dell'organizzazione nella regione corrente. Se l'amministratore delegato abilita automaticamente gli standard predefiniti, tutti i controlli che fanno parte di questi standard vengono abilitati automaticamente anche con parametri predefiniti per i nuovi account dell'organizzazione. Queste impostazioni non si applicano agli account esistenti, quindi è possibile modificare la configurazione dopo che un account si unisce all'organizzazione. La disabilitazione di controlli specifici che fanno parte degli standard predefiniti e la configurazione di standard e controlli aggiuntivi devono essere eseguite separatamente in ogni account e regione.

La configurazione locale non supporta l'uso di politiche di configurazione. Per utilizzare i criteri di configurazione, è necessario passare alla configurazione centrale.

Gestione manuale degli account

Se non integri Security Hub CSPM AWS Organizations o disponi di un account autonomo, devi specificare le impostazioni per ciascun account separatamente in ciascuna regione. La gestione manuale degli account non supporta l'uso di politiche di configurazione.

API di configurazione centralizzate

Operazioni CSPM di Security Hub che solo l'amministratore CSPM delegato di Security Hub CSPM di Security Hub CSPM può utilizzare nella regione di residenza per gestire le politiche di configurazione per gli account gestiti centralmente. Le operazioni includono:

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

Account-specific API

Operazioni CSPM di Security Hub che possono essere utilizzate per abilitare o disabilitare CSPM, standard e controlli di Security Hub account per account. Queste operazioni vengono utilizzate in ogni singola regione.

Self-managed gli account possono utilizzare operazioni specifiche dell'account per configurare le proprie impostazioni. Gli account gestiti centralmente non possono utilizzare le seguenti operazioni specifiche dell'account nella regione di origine e nelle regioni collegate. In tali regioni, solo l'amministratore delegato può configurare gli account gestiti centralmente tramite operazioni di configurazione e politiche di configurazione centralizzate.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

Per verificare lo stato dell'account, il proprietario di un account gestito centralmente può utilizzare `Get` qualsiasi `Describe` operazione dell'API CSPM Security Hub.

Se si utilizza la configurazione locale o la gestione manuale degli account, anziché la configurazione centrale, è possibile utilizzare queste operazioni specifiche dell'account.

Self-managed gli account possono anche utilizzare `*Invitations` e `*Members` operare. Tuttavia, consigliamo che gli account autogestiti non utilizzino queste operazioni. Le associazioni di policy possono fallire se un account membro ha i propri membri che fanno parte di un'organizzazione diversa da quella dell'amministratore delegato.

Unità organizzativa (UO)

In AWS Organizations and Security Hub CSPM, un contenitore per un gruppo di. Account AWS Un'unità organizzativa (OU) può contenere anche altre unità organizzative, il che consente di creare una gerarchia simile a un albero capovolto, con un'unità organizzativa principale nella parte superiore e i rami delle unità organizzative che si estendono verso il basso, terminando con gli account che sono le foglie dell'albero. Un'unità organizzativa può avere esattamente un genitore e ogni account dell'organizzazione può essere membro di una sola unità organizzativa.

È possibile gestire le unità organizzative in AWS Organizations o AWS Control Tower. Per ulteriori informazioni, vedere Gestione delle unità organizzative nella Guida per l'AWS Organizations utente o Gestione di organizzazioni e account AWS Control Tower nella Guida per l'AWS Control Tower utente.

L'amministratore delegato può associare le politiche di configurazione a account o unità organizzative specifici oppure alla directory principale per coprire tutti gli account e le unità organizzative di un'organizzazione.

Gestito centralmente

Un obiettivo che solo l'amministratore delegato può configurare in tutte le regioni utilizzando le politiche di configurazione.

L'account amministratore delegato specifica se una destinazione è gestita centralmente. L'amministratore delegato può anche modificare lo stato di una destinazione da gestita centralmente a gestita automaticamente o viceversa.

Self-managed

Una destinazione che gestisce le proprie impostazioni CSPM di Security Hub. Una destinazione autogestita utilizza operazioni specifiche dell'account per configurare Security Hub CSPM separatamente in ciascuna regione. Ciò è in contrasto con gli obiettivi gestiti centralmente, che sono configurabili solo dall'amministratore delegato in tutte le regioni tramite politiche di configurazione.

L'account amministratore delegato specifica se una destinazione è gestita automaticamente. L'amministratore delegato può applicare un comportamento autogestito a una destinazione. In alternativa, un account o un'unità organizzativa può ereditare il comportamento autogestito da un genitore.

L'account amministratore delegato può essere esso stesso un account autogestito. L'account amministratore delegato può modificare lo stato di una destinazione da autogestito a gestito centralmente o viceversa.

Associazione alla politica di configurazione

Un collegamento tra una politica di configurazione e un account, un'unità organizzativa (OU) o una radice. Quando esiste un'associazione di policy, l'account, l'unità organizzativa o la root utilizza le impostazioni definite dalla politica di configurazione. Esiste un'associazione in uno di questi casi:

- Quando l'amministratore delegato applica direttamente una politica di configurazione a un account, un'unità organizzativa o una directory principale
- Quando un account o un'unità organizzativa eredita una politica di configurazione da un'unità organizzativa principale o dalla directory principale

Un'associazione esiste finché non viene applicata o ereditata una configurazione diversa.

Politica di configurazione applicata

Un tipo di associazione di criteri di configurazione in cui l'amministratore delegato applica direttamente una politica di configurazione agli account di destinazione, alle unità organizzative o alla directory principale. Gli obiettivi sono configurati nel modo definito dalla politica di configurazione e solo l'amministratore delegato può modificarne la configurazione. Se applicata a root, la politica di configurazione influisce su tutti gli account e le unità organizzative dell'organizzazione che non utilizzano una configurazione diversa tramite l'applicazione o l'ereditarietà dal genitore più vicino.

L'amministratore delegato può anche applicare una configurazione autogestita ad account, unità organizzative o root specifici.

Politica di configurazione ereditata

Un tipo di associazione di criteri di configurazione in cui un account o un'unità organizzativa adotta la configurazione dell'unità organizzativa principale o principale più vicina. Se un criterio di configurazione non viene applicato direttamente a un account o a un'unità organizzativa, eredita la configurazione dell'elemento principale più vicino. Tutti gli elementi di una policy vengono ereditati. In altre parole, un account o un'unità organizzativa non possono scegliere di ereditare selettivamente solo parti di una politica. Se il genitore più vicino è autogestito, l'account figlio o l'unità organizzativa eredita il comportamento autogestito del genitore.

L'ereditarietà non può sovrascrivere una configurazione applicata. In altre parole, se un criterio di configurazione o una configurazione autogestita viene applicata direttamente a un account o a un'unità organizzativa, utilizza tale configurazione e non eredita la configurazione dell'unità principale.

Root

In AWS Organizations and Security Hub CSPM, il nodo principale di primo livello di un'organizzazione. Se l'amministratore delegato applica una politica di configurazione a root, la policy viene associata a tutti gli account e le unità organizzative dell'organizzazione, a meno che non utilizzino una politica diversa, tramite applicazione o ereditarietà, o siano designati come autogestiti. Se l'amministratore definisce la directory principale come autogestita, tutti gli account e le unità organizzative dell'organizzazione vengono gestiti automaticamente, a meno che non utilizzino una politica di configurazione tramite l'applicazione o l'ereditarietà. Se la directory principale è gestita automaticamente e al momento non esistono criteri di configurazione, tutti i nuovi account dell'organizzazione mantengono le impostazioni correnti.

I nuovi account che entrano a far parte di un'organizzazione rientrano nella cartella principale finché non vengono assegnati a un'unità organizzativa specifica. Se un nuovo account non viene assegnato a un'unità organizzativa, eredita la configurazione principale a meno che l'amministratore delegato non lo designi come account autogestito.

Abilitazione della configurazione centrale in Security Hub CSPM

L'account amministratore delegato AWS di Security Hub CSPM può utilizzare la configurazione centrale per configurare CSPM, standard e controlli di Security Hub per più account e unità organizzative (OU) in tutto il mondo. Regioni AWS

Per informazioni di base sui vantaggi della configurazione centrale e su come funziona, consulta. Comprendere la configurazione centrale in Security Hub CSPM

Questa sezione spiega i prerequisiti per la configurazione centrale e come iniziare a utilizzarla.

Prerequisiti per la configurazione centrale

Prima di poter iniziare a utilizzare la configurazione centrale, è necessario integrare Security Hub CSPM AWS Organizations e designare una regione di residenza. Se si utilizza la console Security Hub CSPM, questi prerequisiti sono inclusi nel flusso di lavoro di attivazione per la configurazione centrale.

Integrazione con Organizations

È necessario integrare Security Hub CSPM e Organizations per utilizzare la configurazione centrale.

Per integrare questi servizi, è necessario innanzitutto creare un'organizzazione in Organizations. Dall'account di gestione Organizations, si designa quindi un account amministratore delegato CSPM di Security Hub. Per istruzioni, consulta Integrazione del Security Hub CSPM conAWS Organizations.

Assicurati di designare l'amministratore delegato nella regione di residenza desiderata. Quando inizi a utilizzare la configurazione centrale, lo stesso amministratore delegato viene impostato automaticamente anche in tutte le regioni collegate. L'account di gestione Organizations non può essere impostato come account amministratore delegato.

> **Important**
>
> Quando si utilizza la configurazione centrale, non è possibile utilizzare la console CSPM di Security Hub o le API CSPM di Security Hub per modificare o rimuovere

l'account amministratore delegato. Se l'account di gestione Organizations utilizza le AWS Organizations API per modificare o rimuovere l'amministratore delegato di Security Hub CSPM, Security Hub CSPM interrompe automaticamente la configurazione centrale. Inoltre, le policy di configurazione vengono dissociate ed eliminate. Gli account dei membri mantengono la configurazione che avevano prima della modifica o della rimozione dell'amministratore delegato.

Designare una regione d'origine

È necessario designare una regione d'origine per utilizzare la configurazione centralizzata. La regione d'origine è la regione da cui l'amministratore delegato configura l'organizzazione.

> **Note**
>
> La regione d'origine non può essere una regione AWS designata come regione opt-in. Per impostazione predefinita, una regione che prevede l'attivazione è disattivata. Per un elenco delle regioni che hanno aderito, consulta Considerazioni prima di abilitare e disabilitare le regioni nella Guida di riferimento per la gestione degli AWSaccount.

Facoltativamente, puoi specificare una o più regioni collegate configurabili dalla regione di origine.

L'amministratore delegato può creare e gestire le politiche di configurazione solo dalla regione di origine. Le politiche di configurazione hanno effetto nella regione di origine e in tutte le regioni collegate. Non è possibile creare una politica di configurazione che si applichi solo a un sottoinsieme di queste regioni e non ad altre. L'eccezione è rappresentata dai controlli che coinvolgono risorse globali. Se si utilizza la configurazione centrale, Security Hub CSPM disattiva automaticamente i controlli che coinvolgono risorse globali in tutte le regioni tranne la regione di origine. Per ulteriori informazioni, consulta Controlli che utilizzano risorse globali.

La regione di origine è anche la regione di aggregazione CSPM del Security Hub che riceve risultati, approfondimenti e altri dati dalle regioni collegate.

Se hai già impostato una regione di aggregazione per l'aggregazione tra regioni, questa è la tua regione principale predefinita per la configurazione centrale. Puoi modificare la regione di residenza prima di iniziare a utilizzare la configurazione centrale eliminando l'aggregatore di ricerca corrente e creandone uno nuovo nella regione di residenza desiderata. Un aggregatore di risultati è una risorsa CSPM di Security Hub che specifica la regione di origine e le regioni collegate.

Per designare una regione di origine, consulta i passaggi per impostare una regione di aggregazione. Se disponi già di una regione di residenza, puoi richiamare l'GetFindingAggregatorAPI per visualizzarne i dettagli, incluse le regioni attualmente collegate.

Istruzioni per abilitare la configurazione centrale

Scegliete il metodo preferito e seguite i passaggi per abilitare la configurazione centralizzata per la vostra organizzazione.

Security Hub CSPM console

Per abilitare la configurazione centrale (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel pannello di navigazione, scegli Impostazioni e configurazione. Quindi, scegli Avvia configurazione centrale.

   Se stai effettuando l'onboarding su Security Hub CSPM, scegli Vai a Security Hub CSPM.
3. Nella pagina Designare un amministratore delegato, seleziona il tuo account amministratore delegato o inserisci l'ID dell'account. Se applicabile, ti consigliamo di scegliere lo stesso amministratore delegato che hai impostato per altri servizi di AWS sicurezza e conformità. Scegli Imposta amministratore delegato.
4. Nella pagina Centralizza l'organizzazione, nella sezione Regioni, seleziona la tua regione d'origine. Devi aver effettuato l'accesso alla regione d'origine per procedere. Se hai già impostato una regione di aggregazione per l'aggregazione tra regioni, viene visualizzata come regione principale. Per modificare la regione d'origine, scegli Modifica impostazioni della regione. Puoi quindi selezionare la tua regione d'origine preferita e tornare a questo flusso di lavoro.
5. Seleziona almeno una regione da collegare alla regione d'origine. Facoltativamente, scegli se collegare automaticamente le future regioni supportate alla regione d'origine. Le regioni selezionate qui saranno configurabili dalla regione d'origine dall'amministratore delegato. Le politiche di configurazione hanno effetto nella regione di origine e in tutte le regioni collegate.
6. Scegli Conferma e continua.
7. Ora puoi usare la configurazione centrale. Continua a seguire le istruzioni della console per creare la tua prima politica di configurazione. Se non sei ancora pronto per creare una politica di configurazione, scegli Non sono ancora pronto per la configurazione. Puoi creare una politica in un secondo momento scegliendo Impostazioni e configurazione nel

riquadro di navigazione. Per istruzioni sulla creazione di una politica di configurazione, consultaCreazione e associazione di policy di configurazione.

Security Hub CSPM API

Per abilitare la configurazione centrale (API)

1. Utilizzando le credenziali dell'account amministratore delegato, richiama l'UpdateOrganizationConfigurationAPI dalla regione di origine.
2. Imposta il campo su. `AutoEnable` `false`
3. Imposta il `ConfigurationType` campo nell'`OrganizationConfiguration`oggetto su`CENTRAL`. Questa azione ha il seguente impatto:
   - Designa l'account chiamante come amministratore delegato CSPM di Security Hub in tutte le regioni collegate.
   - Abilita Security Hub CSPM nell'account amministratore delegato in tutte le regioni collegate.
   - Designa l'account chiamante come amministratore delegato CSPM di Security Hub per gli account nuovi ed esistenti che utilizzano Security Hub CSPM e appartengono all'organizzazione. Ciò si verifica nella regione d'origine e in tutte le regioni collegate. L'account chiamante viene impostato come amministratore delegato per i nuovi account dell'organizzazione solo se sono associati a una politica di configurazione con Security Hub CSPM abilitato. L'account chiamante viene impostato come amministratore delegato per gli account dell'organizzazione esistenti solo se hanno già abilitato Security Hub CSPM.
   - Viene AutoEnableimpostato su `false` in tutte le regioni collegate e impostato su nella regione AutoEnableStandardsdi origine e `NONE` in tutte le regioni collegate. Questi parametri non sono rilevanti nella home page e nelle regioni collegate quando si utilizza la configurazione centrale, ma è possibile abilitare automaticamente Security Hub CSPM e gli standard di sicurezza predefiniti negli account dell'organizzazione tramite l'uso di policy di configurazione.
4. È ora possibile utilizzare la configurazione centrale. L'amministratore delegato può creare policy di configurazione per configurare Security Hub CSPM nell'organizzazione. Per istruzioni sulla creazione di una politica di configurazione, vedere. Creazione e associazione di policy di configurazione

Esempio di richiesta API:

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

Per abilitare la configurazione centrale (AWS CLI)

1. Utilizzando le credenziali dell'account amministratore delegato, esegui il update-organization-configurationcomando dalla regione di origine.
2. Includere il parametro `no-auto-enable`.
3. Imposta il `ConfigurationType` campo nell'`organization-configuration`oggetto su. `CENTRAL` Questa azione ha il seguente impatto:

   - Designa l'account chiamante come amministratore delegato CSPM di Security Hub in tutte le regioni collegate.
   - Abilita Security Hub CSPM nell'account amministratore delegato in tutte le regioni collegate.
   - Designa l'account chiamante come amministratore delegato CSPM di Security Hub per gli account nuovi ed esistenti che utilizzano Security Hub CSPM e appartengono all'organizzazione. Ciò si verifica nella regione d'origine e in tutte le regioni collegate. L'account chiamante viene impostato come amministratore delegato per i nuovi account dell'organizzazione solo se sono associati a una politica di configurazione con Security Hub abilitato. L'account chiamante viene impostato come amministratore delegato per gli account dell'organizzazione esistenti solo se hanno già abilitato Security Hub CSPM.
   - Imposta l'opzione di attivazione automatica su tutte le regioni collegate e imposta su no-auto-enablenella regione auto-enable-standardsdi origine e `NONE` in tutte le regioni collegate. Questi parametri non sono rilevanti nella home page e nelle regioni collegate quando si utilizza la configurazione centrale, ma è possibile abilitare automaticamente Security Hub CSPM e gli standard di sicurezza predefiniti negli account dell'organizzazione tramite l'uso di policy di configurazione.
4. È ora possibile utilizzare la configurazione centrale. L'amministratore delegato può creare policy di configurazione per configurare Security Hub CSPM nell'organizzazione. Per

istruzioni sulla creazione di una politica di configurazione, vedere. Creazione e associazione di policy di configurazione

Comando di esempio:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

Obiettivi gestiti centralmente e obiettivi autogestiti

Quando si abilita la configurazione centrale, l'amministratore delegato di AWS Security Hub CSPM può designare ogni account dell'organizzazione, unità organizzativa (OU) e root come gestiti centralmente o autogestiti. Il tipo di gestione di una destinazione determina come specificare le relative impostazioni CSPM del Security Hub.

Per informazioni di base sui vantaggi della configurazione centralizzata e su come funziona, consulta. Comprendere la configurazione centrale in Security Hub CSPM

Questa sezione spiega le differenze tra una designazione gestita centralmente e una autogestita e come scegliere il tipo di gestione di un account, di un'unità organizzativa o della directory principale.

Self-managed

Il proprietario di un account, unità organizzativa o root autogestito deve configurarne le impostazioni separatamente in ciascuno di essi. Regione AWS L'amministratore delegato non può creare politiche di configurazione per obiettivi autogestiti.

Gestito centralmente

Solo l'amministratore delegato di Security Hub CSPM può configurare le impostazioni per gli account, le unità organizzative gestite centralmente o la radice nella regione principale e nelle regioni collegate. Le policy di configurazione possono essere associate ad account e unità organizzative gestiti centralmente.

L'amministratore delegato può cambiare lo stato di una destinazione tra gestione automatica e gestione centralizzata. Per impostazione predefinita, tutti gli account e l'unità organizzativa vengono gestiti automaticamente quando si avvia la configurazione centrale tramite l'API CSPM Security Hub.

Nella console, il tipo di gestione dipende dalla prima politica di configurazione. Gli account e le unità organizzative associati alla prima policy vengono gestiti centralmente. Per impostazione predefinita, gli altri account e unità organizzative vengono gestiti automaticamente.

Se si associa una politica di configurazione a un account precedentemente gestito in modo autonomo, le impostazioni dei criteri hanno la precedenza sulla designazione autogestita. L'account viene gestito centralmente e adotta le impostazioni riportate nella politica di configurazione.

Se si modifica un account gestito centralmente in un account autogestito, le impostazioni precedentemente applicate all'account tramite una politica di configurazione rimangono invariate. Ad esempio, un account gestito centralmente potrebbe inizialmente essere associato a una policy che abilitava Security Hub CSPM, abilitava le migliori pratiche di sicurezza AWS di base e disabilitava. CloudTrail.1 Se poi si designa l'account come autogestito, tutte le impostazioni rimangono invariate. Tuttavia, il proprietario dell'account può modificare autonomamente le impostazioni dell'account in futuro.

Gli account figli e le unità organizzative possono ereditare il comportamento autogestito da un genitore autogestito, allo stesso modo in cui gli account figli e le unità organizzative possono ereditare le politiche di configurazione da un genitore gestito centralmente. Per ulteriori informazioni, consulta Associazione delle politiche tramite applicazione ed ereditarietà.

Un account o un'unità organizzativa autogestiti non possono ereditare una politica di configurazione da un nodo principale o dalla radice. Ad esempio, se si desidera che tutti gli account e le unità organizzative dell'organizzazione ereditino una politica di configurazione dalla radice, è necessario modificare il tipo di gestione dei nodi autogestiti in gestione centralizzata.

Opzioni per configurare le impostazioni negli account autogestiti

Self-managed gli account devono configurare le proprie impostazioni separatamente in ciascuna regione.

I proprietari di account autogestiti possono richiamare le seguenti operazioni dell'API CSPM Security Hub in ciascuna regione per configurare le proprie impostazioni:

- `EnableSecurityHube DisableSecurityHub` per abilitare o disabilitare il servizio CSPM di Security Hub (se un account autogestito ha un amministratore CSPM di Security Hub delegato, l'amministratore deve dissociare l'account prima che il proprietario dell'account possa disabilitare Security Hub CSPM).
- `BatchEnableStandardse BatchDisableStandards` per abilitare o disabilitare gli standard

- `BatchUpdateStandardsControlAssociations`o `UpdateStandardsControl` per abilitare o disabilitare i controlli

Self-managed gli account possono anche utilizzare `*Invitations` e `*Members` operare. Tuttavia, consigliamo che gli account autogestiti non utilizzino queste operazioni. Le associazioni di policy possono fallire se un account membro ha i propri membri che fanno parte di un'organizzazione diversa da quella dell'amministratore delegato.

Per le descrizioni delle azioni dell'API CSPM di Security Hub, vedere il riferimento all'API CSPM AWS di Security Hub.

Self-managed gli account possono anche utilizzare la console CSPM di Security Hub o AWS CLI configurare le proprie impostazioni in ciascuna regione.

Self-managed gli account non possono richiamare alcuna API relativa ai criteri di configurazione e alle associazioni di policy di Security Hub CSPM. Solo l'amministratore delegato può richiamare le API di configurazione centrale e utilizzare le politiche di configurazione per configurare account gestiti centralmente.

Scelta del tipo di gestione di una destinazione

Scegli il tuo metodo preferito e segui i passaggi per designare un account o un'unità organizzativa come gestito centralmente o autogestito in AWS Security Hub CSPM.

Security Hub CSPM console

Per scegliere il tipo di gestione di un account o di un'unità organizzativa

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore CSPM di Security Hub delegato nella regione di residenza.
2. Scegliere Configuration (Configurazione).
3. Nella scheda Organizzazione, seleziona l'account o l'unità organizzativa di destinazione. Scegli Modifica.
4. Nella pagina Definisci configurazione, per Tipo di gestione, scegli Gestito centralmente se desideri che l'amministratore delegato configuri l'account o l'unità organizzativa di destinazione. Quindi, scegli Applica una politica specifica se desideri associare una politica di

configurazione esistente alla destinazione. Scegli Inherit from my organization se desideri che il target erediti la configurazione del genitore più vicino. Scegli Self-managedse desideri che l'account o l'unità organizzativa configurino le proprie impostazioni.

5. Scegli Next (Successivo). Controlla le modifiche e scegli Salva.

Security Hub CSPM API

Per scegliere il tipo di gestione di un account o di un'unità organizzativa

1. Richiama l'StartConfigurationPolicyAssociationAPI dall'account amministratore delegato CSPM di Security Hub nella regione di origine.
2. Per il `ConfigurationPolicyIdentifier` campo, specifica `SELF_MANAGED_SECURITY_HUB` se desideri che l'account o l'unità organizzativa controllino le proprie impostazioni. Fornisci l'Amazon Resource Name (ARN) o l'ID della politica di configurazione pertinente se desideri che l'amministratore delegato controlli le impostazioni dell'account o dell'unità organizzativa.
3. Per il `Target` campo, fornisci l'Account AWSID, l'ID OU o l'ID root della destinazione di cui desideri modificare il tipo di gestione. Ciò associa il comportamento autogestito o la politica di configurazione specificata alla destinazione. Gli account secondari della destinazione possono ereditare il comportamento autogestito o la politica di configurazione.

Esempio di richiesta API per designare un account autogestito:

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Per scegliere il tipo di gestione di un account o di un'unità organizzativa

1. Esegui il start-configuration-policy-associationcomando dall'account amministratore delegato CSPM di Security Hub nella regione di origine.
2. Per `configuration-policy-identifier` campo, specifica `SELF_MANAGED_SECURITY_HUB` se desideri che l'account o l'unità organizzativa controllino

le proprie impostazioni. Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione pertinente se desideri che l'amministratore delegato controlli le impostazioni dell'account o dell'unità organizzativa.

3. Per il `target` campo, fornisci l'Account AWSID, l'ID OU o l'ID root della destinazione di cui desideri modificare il tipo di gestione. Ciò associa il comportamento autogestito o la politica di configurazione specificata alla destinazione. Gli account secondari della destinazione possono ereditare il comportamento autogestito o la politica di configurazione.

Esempio di comando per designare un account autogestito:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Come funzionano le politiche di configurazione in Security Hub CSPM

L'amministratore delegato AWS di Security Hub CSPM può creare policy di configurazione per configurare Security Hub CSPM, standard di sicurezza e controlli di sicurezza per un'organizzazione. Dopo aver creato una politica di configurazione, l'amministratore delegato può associarla ad account, unità organizzative (OU) specifici o alla directory principale. La politica ha quindi effetto negli account, nelle unità organizzative o nella directory principale specificati.

Per informazioni di base sui vantaggi della configurazione centralizzata e su come funziona, consultaComprendere la configurazione centrale in Security Hub CSPM.

Questa sezione fornisce una panoramica dettagliata delle politiche di configurazione.

Considerazioni sulle politiche

Prima di creare una politica di configurazione in Security Hub CSPM, considera i seguenti dettagli.

- Le politiche di configurazione devono essere associate per avere effetto: dopo aver creato una politica di configurazione, è possibile associarla a uno o più account, unità organizzative (OU) o root. Una politica di configurazione può essere associata agli account o alle unità organizzative tramite applicazione diretta o tramite ereditarietà da un'unità organizzativa principale.
- Un account o un'unità organizzativa possono essere associati a una sola politica di configurazione: per evitare conflitti di impostazioni, un account o un'unità organizzativa può essere associato a una

sola politica di configurazione alla volta. In alternativa, un account o un'unità organizzativa possono essere gestiti automaticamente.

- I criteri di configurazione sono completi: i criteri di configurazione forniscono una specifica completa delle impostazioni. Ad esempio, un account figlio non può accettare impostazioni per alcuni controlli da un criterio e impostazioni per altri controlli da un altro criterio. Quando associ una politica a un account per bambini, assicurati che la politica specifichi tutte le impostazioni che desideri che l'account per bambini utilizzi.
- I criteri di configurazione non possono essere ripristinati: non è possibile ripristinare un criterio di configurazione dopo averlo associato ad account o unità organizzative. Ad esempio, se si associa una politica di configurazione che disabilita CloudWatch i controlli a un account specifico e poi si dissocia tale politica, i CloudWatch controlli continuano a essere disabilitati in quell'account. Per abilitare nuovamente CloudWatch i controlli, puoi associare l'account a una nuova politica che abilita i controlli. In alternativa, puoi modificare l'account rendendolo autogestito e abilitare ogni CloudWatch controllo nell'account.
- I criteri di configurazione hanno effetto nella regione di origine e in tutte le regioni collegate: i criteri di configurazione hanno effetto su tutti gli account associati nella regione di origine e in tutte le regioni collegate. Non è possibile creare una politica di configurazione che abbia effetto solo in alcune di queste regioni e non in altre. L'eccezione è rappresentata dai controlli che utilizzano risorse globali. Security Hub CSPM disattiva automaticamente i controlli che coinvolgono risorse globali in tutte le regioni tranne la regione di origine.

  Le regioni AWS introdotte a partire dal 20 marzo 2019 sono note come regioni opt-in. È necessario abilitare tale regione per un account prima che una politica di configurazione abbia effetto su tale account. L'account di gestione Organizations può abilitare le regioni opzionali per un account membro. Per istruzioni sull'attivazione delle regioni che richiedono l'iscrizione, consulta Specificare quali possono essere utilizzate dal Regioni AWS tuo account nella Guida di riferimento per la gestione degli AWS account.

  Se la tua politica configura un controllo che non è disponibile nella regione di origine o in una o più aree collegate, Security Hub CSPM salta la configurazione del controllo nelle regioni non disponibili ma applica la configurazione nelle regioni in cui il controllo è disponibile. Ti manca la copertura necessaria per un controllo che non è disponibile nella regione d'origine o in nessuna delle aree collegate.
- Le policy di configurazione sono risorse: come risorsa, una policy di configurazione ha un Amazon Resource Name (ARN) e un identificatore univoco universale (UUID). L'ARN utilizza il seguente formato:. `arn:partition:securityhub:region:delegated administrator`

account ID:configuration-policy/*configuration policy UUID* Una configurazione autogestita non ha ARN o UUID. L'identificatore per una configurazione autogestita è. SELF_MANAGED_SECURITY_HUB

- Gli standard multicloud non sono supportati nelle politiche di configurazione: le politiche di configurazione possono includere solo standard e controlli di AWS sicurezza. Gli standard multicloud, come CIS Azure Foundations Benchmark v4.0.0, e i relativi controlli associati (ad esempio) non possono essere inclusi in una politica di configurazione. Azure.Storage.1 Se includi un ARN o un ID di controllo standard multicloud in una politica di configurazione, la richiesta restituisce un. InvalidInputException Per abilitare o configurare gli standard multicloud, utilizza i meccanismi di configurazione locali direttamente nel file desiderato. Account AWS

Tipi di politiche di configurazione

Ogni politica di configurazione specifica le seguenti impostazioni:

- Abilita o disabilita Security Hub CSPM.
- Abilita uno o più standard di sicurezza.
- Indica quali controlli di sicurezza sono abilitati negli standard abilitati. È possibile farlo fornendo un elenco di controlli specifici che devono essere abilitati e Security Hub CSPM disabilita tutti gli altri controlli, inclusi i nuovi controlli quando vengono rilasciati. In alternativa, puoi fornire un elenco di controlli specifici che devono essere disabilitati e Security Hub CSPM abilita tutti gli altri controlli, inclusi i nuovi controlli quando vengono rilasciati.
- Facoltativamente, personalizza i parametri per selezionare i controlli abilitati tra gli standard abilitati.

Le politiche di configurazione centrale non includono le impostazioni del AWS Config registratore. È necessario abilitare AWS Config e attivare separatamente la registrazione per le risorse richieste affinché Security Hub CSPM generi i risultati del controllo. Per ulteriori informazioni, consulta Considerazioni prima dell'attivazione e della configurazione AWS Config.

Se si utilizza la configurazione centrale, Security Hub CSPM disattiva automaticamente i controlli che coinvolgono risorse globali in tutte le regioni tranne la regione di origine. Gli altri controlli che scegli di abilitare tramite una politica di configurazione sono abilitati in tutte le regioni in cui sono disponibili. Per limitare i risultati di questi controlli a una sola regione, puoi aggiornare le impostazioni del AWS Config registratore e disattivare la registrazione globale delle risorse in tutte le regioni tranne la regione d'origine.

Se un controllo abilitato che coinvolge risorse globali non è supportato nella regione di origine, Security Hub CSPM tenta di abilitare il controllo in una regione collegata in cui il controllo è supportato. Con la configurazione centralizzata, ti manca la copertura per un controllo che non è disponibile nella regione d'origine o in nessuna delle regioni collegate.

Per un elenco dei controlli che coinvolgono risorse globali, consultaControlli che utilizzano risorse globali.

Politica di configurazione consigliata

Quando si crea una politica di configurazione per la prima volta nella console CSPM di Security Hub, è possibile scegliere la politica consigliata da Security Hub CSPM.

La policy consigliata abilita Security Hub CSPM, lo standard AWS Foundational Security Best Practices (FSBP) e tutti i controlli FSBP esistenti e nuovi. I controlli che accettano i parametri utilizzano i valori predefiniti. La politica consigliata si applica a root (tutti gli account e le unità organizzative, sia nuovi che esistenti). Dopo aver creato la politica consigliata per l'organizzazione, è possibile modificarla dall'account amministratore delegato. Ad esempio, puoi abilitare standard o controlli aggiuntivi o disabilitare controlli FSBP specifici. Per istruzioni sulla modifica di una politica di configurazione, consulta. Aggiornamento delle politiche di configurazione

Politica di configurazione personalizzata

Invece della politica consigliata, l'amministratore delegato può creare fino a 20 politiche di configurazione personalizzate. È possibile associare una singola politica personalizzata all'intera organizzazione o diverse politiche personalizzate a diversi account e unità organizzative. Per una politica di configurazione personalizzata, è necessario specificare le impostazioni desiderate. Ad esempio, puoi creare una policy personalizzata che abiliti FSBP, il Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 e tutti i controlli di tali standard tranne i controlli Amazon Redshift. Il livello di granularità utilizzato nelle politiche di configurazione personalizzate dipende dall'ambito di copertura di sicurezza previsto in tutta l'organizzazione.

> **Note**
>
> Non è possibile associare una politica di configurazione che disabiliti Security Hub CSPM all'account amministratore delegato. Tale politica può essere associata ad altri account ma ignora l'associazione con l'amministratore delegato. L'account amministratore delegato mantiene la configurazione corrente.

Dopo aver creato una politica di configurazione personalizzata, è possibile passare alla politica di configurazione consigliata aggiornando la politica di configurazione in modo che rifletta la configurazione consigliata. Tuttavia, non è possibile scegliere di creare la politica di configurazione consigliata nella console CSPM di Security Hub dopo la creazione della prima politica.

Associazione delle politiche tramite applicazione ed ereditarietà

Quando si attiva per la prima volta la configurazione centrale, l'organizzazione non ha associazioni e si comporta nello stesso modo in cui si comportava prima dell'opt-in. L'amministratore delegato può quindi stabilire associazioni tra una politica di configurazione o un comportamento autogestito e gli account, le unità organizzative o la directory principale. Le associazioni possono essere stabilite tramite applicazione o ereditarietà.

Dall'account amministratore delegato, è possibile applicare direttamente una politica di configurazione a un account, a un'unità organizzativa o alla radice. In alternativa, l'amministratore delegato può applicare direttamente una designazione autogestita a un account, a un'unità organizzativa o alla directory principale.

In assenza di un'applicazione diretta, un account o un'unità organizzativa eredita le impostazioni del genitore più vicino che ha una politica di configurazione o un comportamento autogestito. Se il genitore più prossimo è associato a una politica di configurazione, il figlio eredita tale politica ed è configurabile solo dall'amministratore delegato della regione di origine. Se il genitore più prossimo è autogestito, il figlio eredita il comportamento autogestito e ha la possibilità di specificare le proprie impostazioni in ciascuno di essi. Regione AWS

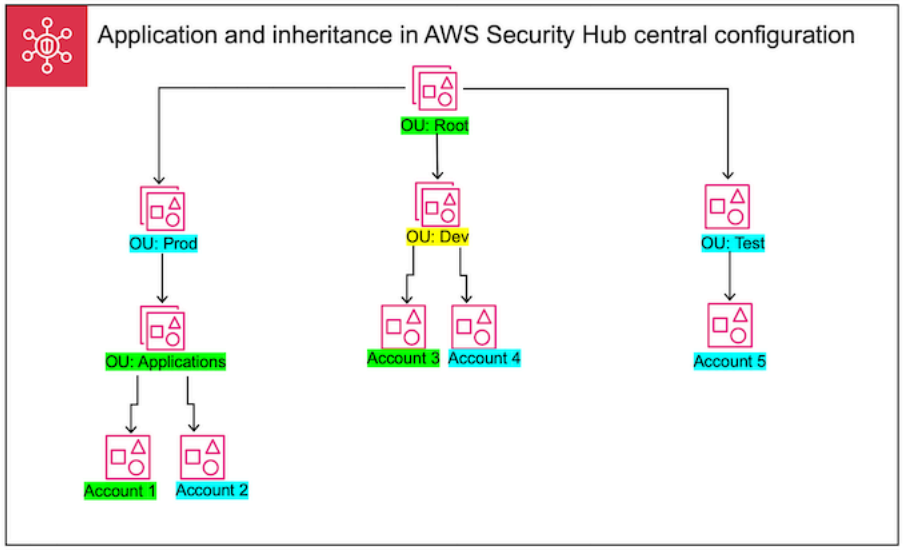
L'applicazione ha la precedenza sull'ereditarietà. In altre parole, l'ereditarietà non sostituisce una politica di configurazione o una designazione autogestita che l'amministratore delegato ha applicato direttamente a un account o a un'unità organizzativa.

Se si applica direttamente un criterio di configurazione a un account autogestito, il criterio ha la precedenza sulla designazione autogestita. L'account viene gestito centralmente e adotta le impostazioni riportate nella politica di configurazione.

Si consiglia di applicare direttamente una politica di configurazione alla radice. Se applichi una policy alla root, i nuovi account che entrano a far parte dell'organizzazione erediteranno automaticamente la policy principale, a meno che non li associ a una politica diversa o non li definiate come autogestiti.

È possibile associare una sola politica di configurazione a un account o a un'unità organizzativa alla volta, tramite applicazione o ereditarietà. Questo è progettato per evitare conflitti di impostazioni.

Il diagramma seguente illustra come funzionano l'applicazione delle politiche e l'ereditarietà nella configurazione centrale.



In questo esempio, a un nodo evidenziato in verde è stata applicata una politica di configurazione. A un nodo evidenziato in blu non è stata applicata alcuna politica di configurazione. Un nodo evidenziato in giallo è stato designato come autogestito. Ogni account e unità organizzativa utilizza la seguente configurazione:

- OU:Root (Verde): questa unità organizzativa utilizza la politica di configurazione che le è stata applicata.
- OU:Prod (Blu): questa unità organizzativa eredita la politica di configurazione da OU:Root.
- OU:Applications (Verde): questa unità organizzativa utilizza la politica di configurazione che le è stata applicata.
- Account 1 (verde): questo account utilizza la politica di configurazione che gli è stata applicata.
- Account 2 (blu): questo account eredita la politica di configurazione da OU:Applications.
- OU:Dev (Giallo): questa unità organizzativa è gestita automaticamente.
- Account 3 (verde): questo account utilizza la politica di configurazione che gli è stata applicata.
- Account 4 (blu): questo account eredita il comportamento autogestito da. OU:Dev
- OU:Test (Blu): questo account eredita la politica di configurazione da. OU:Root
- Account 5 (blu): questo account eredita la politica di configurazione OU:Root dal momento che il suo genitore diretto non è associato a una politica di configurazione. OU:Test

Test di una politica di configurazione

Per assicurarti di comprendere come funzionano le politiche di configurazione, ti consigliamo di creare una policy e di associarla a un account di prova o a un'unità organizzativa.

Per testare una politica di configurazione

1. Crea una politica di configurazione personalizzata e verifica che le impostazioni specificate per l'abilitazione, gli standard e i controlli di Security Hub CSPM siano corretti. Per istruzioni, consulta Creazione e associazione di policy di configurazione.
2. Applica la politica di configurazione a un account di test o a un'unità organizzativa che non dispone di account secondari o unità organizzative.
3. Verifica che l'account di test o l'unità organizzativa utilizzi la politica di configurazione nel modo previsto nella tua regione di origine e in tutte le regioni collegate. Puoi anche verificare che tutti gli altri account e unità organizzative dell'organizzazione rimangano autogestiti e che sia possibile modificare le proprie impostazioni in ciascuna regione.

Dopo aver testato una politica di configurazione in un singolo account o unità organizzativa, è possibile associarla ad altri account e unità organizzative.

Creazione e associazione di policy di configurazione

L'account amministratore delegato AWS di Security Hub CSPM può creare policy di configurazione che specificano come i CSPM, gli standard e i controlli di Security Hub sono configurati in account e unità organizzative (OU) specifici. Una politica di configurazione ha effetto solo dopo che l'amministratore delegato la associa ad almeno un account o unità organizzativa (OU) o alla radice. L'amministratore delegato può anche associare una configurazione autogestita agli account, alle unità organizzative o alla radice.

Se è la prima volta che crei una politica di configurazione, ti consigliamo di esaminarla prima. Come funzionano le politiche di configurazione in Security Hub CSPM

> **Note**
>
> Le policy di configurazione supportano solo AWS standard e controlli. Non è possibile includere standard multicloud (come CIS Azure Foundations Benchmark v4.0.0) o controlli di Azure in una policy di configurazione. Inclusi un ARN standard multicloud o restituzioni di ID

di controllo. `InvalidInputException` Per abilitare o configurare gli standard multicloud, utilizza i meccanismi di configurazione locali direttamente nell'area desiderata. Account AWS

Scegli il metodo di accesso preferito e segui i passaggi per creare e associare una politica di configurazione o una configurazione autogestita. Quando si utilizza la console Security Hub CSPM, è possibile associare una configurazione a più account o unità organizzative contemporaneamente. Quando si utilizza l'API CSPM di Security Hub AWS CLI, è possibile associare una configurazione a un solo account o unità organizzativa in ogni richiesta.

> **Note**
>
> Se si utilizza la configurazione centrale, Security Hub CSPM disattiva automaticamente i controlli che coinvolgono risorse globali in tutte le regioni tranne la regione di origine. Gli altri controlli che scegli di abilitare tramite una politica di configurazione sono abilitati in tutte le regioni in cui sono disponibili. Per limitare i risultati di questi controlli a una sola regione, puoi aggiornare le impostazioni del AWS Config registratore e disattivare la registrazione globale delle risorse in tutte le regioni tranne la regione d'origine.
> Se un controllo abilitato che coinvolge risorse globali non è supportato nella regione di origine, Security Hub CSPM tenta di abilitare il controllo in una regione collegata in cui il controllo è supportato. Con la configurazione centralizzata, ti manca la copertura per un controllo che non è disponibile nella regione d'origine o in nessuna delle regioni collegate.
> Per un elenco dei controlli che coinvolgono risorse globali, consultaControlli che utilizzano risorse globali.

Security Hub CSPM console

Per creare e associare politiche di configurazione

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore CSPM di Security Hub delegato nella regione di residenza.
2. Nel riquadro di navigazione, scegli Configurazione e la scheda Politiche. Quindi, scegli Crea politica.

3. Nella pagina Configura organizzazione, se è la prima volta che crei una politica di configurazione, vedi tre opzioni in Tipo di configurazione. Se hai già creato almeno una politica di configurazione, vedi solo l'opzione Politica personalizzata.

   - Scegli Usa la configurazione CSPM AWS consigliata di Security Hub in tutta la mia organizzazione per utilizzare la nostra politica consigliata. La politica consigliata abilita Security Hub CSPM in tutti gli account dell'organizzazione, abilita lo standard AWS Foundational Security Best Practices (FSBP) e abilita tutti i controlli FSBP nuovi ed esistenti. I controlli utilizzano i valori dei parametri predefiniti.
   - Scegli Non sono ancora pronto a configurare per creare una politica di configurazione in un secondo momento.
   - Scegli Politica personalizzata per creare una politica di configurazione personalizzata. Specificare se abilitare o disabilitare Security Hub CSPM, quali standard abilitare e quali controlli abilitare in base a tali standard. Facoltativamente, specifica i valori dei parametri personalizzati per uno o più controlli abilitati che supportano i parametri personalizzati.

4. Nella sezione Account, scegli gli account di destinazione, le unità organizzative o la radice a cui desideri applicare la politica di configurazione.

   - Scegli Tutti gli account se desideri applicare la politica di configurazione alla radice. Ciò include tutti gli account e le unità organizzative dell'organizzazione a cui non è stata applicata o ereditata un'altra politica.
   - Scegli Account specifici se desideri applicare la politica di configurazione a account o unità organizzative specifici. Inserisci gli ID degli account o seleziona gli account e le unità organizzative dalla struttura dell'organizzazione. È possibile applicare la policy a un massimo di 15 destinazioni (account, unità organizzative o root) al momento della creazione. Per specificare un numero maggiore, modifica la policy dopo la creazione e applicala a obiettivi aggiuntivi.
   - Scegli Solo l'amministratore delegato per applicare la politica di configurazione all'account amministratore delegato corrente.

5. Scegli Next (Successivo).

6. Nella pagina Rivedi e applica, esamina i dettagli della politica di configurazione. Quindi, scegli Crea politica e applica. Nella tua regione d'origine e nelle aree collegate, questa azione sostituisce le impostazioni di configurazione esistenti degli account associati a questa politica di configurazione. Gli account possono essere associati alla politica di configurazione tramite l'applicazione o l'ereditarietà da un nodo principale. Gli account secondari e le unità organizzative delle destinazioni applicate erediteranno automaticamente questa politica di

configurazione a meno che non vengano specificamente esclusi, gestiti automaticamente o utilizzino una politica di configurazione diversa.

Security Hub CSPM API

Per creare e associare politiche di configurazione

1. Richiama l'CreateConfigurationPolicyAPI dall'account amministratore delegato CSPM di Security Hub nella regione di origine.
2. PerName, fornisci un nome univoco per la politica di configurazione. FacoltativamenteDescription, fornisci una descrizione per la politica di configurazione.
3. Per il `ServiceEnabled` campo, specificare se si desidera che Security Hub CSPM sia abilitato o disabilitato in questa politica di configurazione.
4. Per il `EnabledStandardIdentifiers` campo, specificare gli standard CSPM di Security Hub che si desidera abilitare in questa politica di configurazione.
5. Per l'`SecurityControlsConfiguration`oggetto, specifica quali controlli vuoi abilitare o disabilitare in questa politica di configurazione. La scelta `EnabledSecurityControlIdentifiers` significa che i controlli specificati sono abilitati. Gli altri controlli che fanno parte degli standard abilitati (inclusi i controlli appena rilasciati) sono disabilitati. La scelta `DisabledSecurityControlIdentifiers` significa che i controlli specificati sono disabilitati. Gli altri controlli che fanno parte degli standard abilitati (inclusi i controlli appena rilasciati) sono abilitati.
6. Facoltativamente, per il `SecurityControlCustomParameters` campo, specificate i controlli abilitati per i quali desiderate personalizzare i parametri. `CUSTOM`Specificate il `ValueType` campo e il valore del parametro personalizzato per il `Value` campo. Il valore deve essere il tipo di dati corretto e rientrare negli intervalli validi specificati da Security Hub CSPM. Solo i controlli selezionati supportano valori di parametri personalizzati. Per ulteriori informazioni, consulta Comprensione dei parametri di controllo in Security Hub CSPM.
7. Per applicare i criteri di configurazione agli account o alle unità organizzative, richiama l'StartConfigurationPolicyAssociationAPI dall'account amministratore delegato CSPM di Security Hub nella regione di origine.
8. Per il `ConfigurationPolicyIdentifier` campo, fornisci l'Amazon Resource Name (ARN) o l'identificatore univoco universale (UUID) della politica. L'ARN e l'UUID vengono restituiti dall'API. `CreateConfigurationPolicy` Per una configurazione autogestita, il `ConfigurationPolicyIdentifier` campo è uguale a. `SELF_MANAGED_SECURITY_HUB`

9. Per il `Target` campo, fornisci l'unità organizzativa, l'account o l'ID root a cui desideri applicare questa politica di configurazione. È possibile fornire un solo obiettivo in ogni richiesta API. Gli account secondari e le unità organizzative della destinazione selezionata erediteranno automaticamente questa politica di configurazione, a meno che non vengano gestiti automaticamente o utilizzino una politica di configurazione diversa.

Esempio di richiesta API per creare una politica di configurazione:

```
{
    "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
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Esempio di richiesta API per associare una politica di configurazione:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

Per creare e associare politiche di configurazione

1. Esegui il create-configuration-policycomando dall'account amministratore delegato CSPM di Security Hub nella regione di origine.
2. Pername, fornisci un nome univoco per la politica di configurazione. Facoltativamentedescription, fornisci una descrizione per la politica di configurazione.
3. Per il `ServiceEnabled` campo, specificare se si desidera che Security Hub CSPM sia abilitato o disabilitato in questa politica di configurazione.
4. Per il `EnabledStandardIdentifiers` campo, specificare gli standard CSPM di Security Hub che si desidera abilitare in questa politica di configurazione.
5. Per il `SecurityControlsConfiguration` campo, specifica quali controlli vuoi abilitare o disabilitare in questa politica di configurazione. La scelta `EnabledSecurityControlIdentifiers` significa che i controlli specificati sono abilitati. Gli altri controlli che fanno parte degli standard abilitati (inclusi i controlli appena rilasciati) sono disabilitati. La scelta `DisabledSecurityControlIdentifiers` significa che i controlli specificati sono disabilitati. Gli altri controlli che si applicano agli standard abilitati (inclusi i controlli appena rilasciati) sono abilitati.
6. Facoltativamente, per il `SecurityControlCustomParameters` campo, specificate i controlli abilitati per i quali desiderate personalizzare i parametri. `CUSTOM`Specificate il `ValueType` campo e il valore del parametro personalizzato per il `Value` campo. Il valore deve essere il tipo di dati corretto e rientrare negli intervalli validi specificati da Security Hub CSPM. Solo i controlli selezionati supportano valori di parametri personalizzati. Per ulteriori informazioni, consulta Comprensione dei parametri di controllo in Security Hub CSPM.

7. Per applicare i criteri di configurazione agli account o alle unità organizzative, esegui il start-configuration-policy-associationcomando dall'account amministratore delegato CSPM di Security Hub nell'area di residenza.
8. Per il `configuration-policy-identifier` campo, fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione. L'ARN e l'ID vengono restituiti dal `create-configuration-policy` comando.
9. Per il `target` campo, fornisci l'unità organizzativa, l'account o l'ID root a cui desideri applicare questa politica di configurazione. È possibile fornire un solo obiettivo ogni volta che si esegue il comando. I figli della destinazione selezionata erediteranno automaticamente questa politica di configurazione a meno che non si gestiscano autonomamente o utilizzino una politica di configurazione diversa.

Comando di esempio per creare una politica di configurazione:

```
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}}}}]}}}'
```

Comando di esempio per associare una politica di configurazione:

```
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"}'
```

L'`StartConfigurationPolicyAssociation`API restituisce un campo chiamato`AssociationStatus`. Questo campo indica se un'associazione di politiche è in sospeso o in uno stato di successo o di fallimento. La modifica dello stato da a `SUCCESS` o `FAILURE`

può richiedere fino a 24 ore. `PENDING` Per ulteriori informazioni sullo stato dell'associazione, vedereRevisione dello stato di associazione di una politica di configurazione.

Revisione dello stato e dei dettagli delle politiche di configurazione

L'amministratore delegato AWS di Security Hub CSPM può visualizzare le politiche di configurazione per un'organizzazione e i relativi dettagli. Ciò include gli account e le unità organizzative (OU) a cui è associata una politica.

Per informazioni di base sui vantaggi della configurazione centralizzata e su come funziona, consultaComprendere la configurazione centrale in Security Hub CSPM.

Scegliete il metodo preferito e seguite i passaggi per visualizzare le vostre politiche di configurazione.

Security Hub CSPM console

Per visualizzare le politiche di configurazione (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore CSPM di Security Hub delegato nella regione di residenza.
2. Nel riquadro di navigazione, scegli Impostazioni e configurazione.
3. Scegli la scheda Politiche per una panoramica delle tue politiche di configurazione.
4. Seleziona una politica di configurazione e scegli Visualizza dettagli per visualizzare ulteriori dettagli al riguardo, inclusi gli account e le unità organizzative a cui è associata.

Security Hub CSPM API

Per visualizzare un elenco riepilogativo di tutte le politiche di configurazione, utilizza il ListConfigurationPoliciesfunzionamento dell'API CSPM Security Hub. Se usi ilAWS CLI, esegui il comando. list-configuration-policies L'account amministratore delegato di Security Hub CSPM deve richiamare l'operazione nella regione di origine.

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

Per visualizzare i dettagli su una politica di configurazione specifica, usa l'operazione. GetConfigurationPolicy Se usi ilAWS CLI, esegui il get-configuration-policy. L'account amministratore delegato deve richiamare l'operazione nella regione di origine. Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione di cui desideri visualizzare i dettagli.

```
$ aws securityhub get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Per visualizzare un elenco riepilogativo di tutte le politiche di configurazione e le relative associazioni di account, utilizza l'ListConfigurationPolicyAssociationsoperazione. Se usi ilAWS CLI, esegui il list-configuration-policy-associationscomando. L'account amministratore delegato deve richiamare l'operazione nella regione di origine. Facoltativamente, è possibile fornire parametri di impaginazione o filtrare i risultati in base a un ID di policy specifico, al tipo di associazione o allo stato dell'associazione.

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

Per visualizzare le associazioni per un account specifico, utilizzare l'GetConfigurationPolicyAssociationoperazione. Se si utilizza ilAWS CLI, eseguire il get-configuration-policy-associationcomando. L'account amministratore delegato deve richiamare l'operazione nella regione di origine. Per`target`, fornisci il numero di account, l'ID dell'unità organizzativa o l'ID root.

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

Revisione dello stato di associazione di una politica di configurazione

Le seguenti operazioni API di configurazione centrale restituiscono un campo chiamato`AssociationStatus`:

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Questo campo viene restituito sia quando la configurazione sottostante è una politica di configurazione sia quando si tratta di un comportamento autogestito.

Il valore di `AssociationStatus` indica se un'associazione di policy è in sospeso o in stato di successo o di fallimento per un account specifico. La modifica dello stato da a `SUCCESS` o `FAILED` può richiedere fino a 24 ore. `PENDING` Uno stato di `SUCCESS` indica che tutte le impostazioni specificate nella politica di configurazione sono associate all'account. Lo stato di `FAILED` indica che una o più impostazioni specificate nella politica di configurazione non sono state associate all'account. Nonostante `FAILED` lo stato, l'account potrebbe essere parzialmente configurato in base alla politica. Ad esempio, potresti provare ad associare un account a una politica di configurazione che abiliti Security Hub CSPM, abiliti AWS Foundational Security Best Practices e disabiliti. CloudTrail.1 Le due impostazioni iniziali potrebbero avere esito positivo, ma l' CloudTrail.1impostazione potrebbe fallire. In questo esempio, lo stato dell'associazione è valido `FAILED` anche se alcune impostazioni sono state configurate correttamente.

Lo stato di associazione di un'unità organizzativa principale o della radice dipende dallo stato dei relativi figli. Se lo status di associazione di tutti i figli è`SUCCESS`, lo stato dell'associazione del genitore è`SUCCESS`. Se lo status dell'associazione di uno o più figli è`FAILED`, lo stato dell'associazione del genitore è`FAILED`.

Il valore di `AssociationStatus` dipende dallo status di associazione della politica in tutte le regioni pertinenti. Se l'associazione ha successo nella regione d'origine e in tutte le regioni collegate, il valore di `AssociationStatus` è`SUCCESS`. Se l'associazione fallisce in una o più di queste regioni, il valore di `AssociationStatus` è`FAILED`.

Il seguente comportamento influisce anche sul valore di`AssociationStatus`:

- Se la destinazione è un'unità organizzativa principale o la radice, ha uno stato `AssociationStatus` of `SUCCESS` o `FAILED` solo quando tutti i figli hanno uno `FAILED` stato `SUCCESS` or. Se lo stato di associazione di un account figlio o di un'unità organizzativa cambia (ad esempio, quando viene aggiunta o rimossa una regione collegata) dopo aver associato per la prima volta l'account principale a una configurazione, la modifica non aggiorna lo stato di associazione dell'unità principale a meno che non si richiami nuovamente l'`StartConfigurationPolicyAssociation`API.
- Se la destinazione è un account, ha un `AssociationStatus` `SUCCESS` o o `FAILED` solo se l'associazione ha un risultato nella regione d'`SUCCESS`origine e `FAILED` in tutte le regioni collegate. Se lo stato dell'associazione di un account di destinazione cambia (ad esempio, quando viene aggiunta o rimossa una regione collegata) dopo averlo associato per la prima

volta a una configurazione, lo stato dell'associazione viene aggiornato. Tuttavia, la modifica non aggiorna lo stato dell'associazione del genitore a meno che non si richiami nuovamente l'`StartConfigurationPolicyAssociation`API.

Se aggiungi una nuova regione collegata, Security Hub CSPM replica le associazioni esistenti che si trovano in una `PENDING` o in `FAILED` uno stato della nuova regione. `SUCCESS`

Anche quando lo status di associazione è lo`SUCCESS`, lo stato di abilitazione di uno standard che fa parte della politica può passare a uno stato incompleto. In tal caso, Security Hub CSPM non può generare risultati per i controlli dello standard. Per ulteriori informazioni, consulta Verifica dello stato di uno standard.

Risoluzione dei problemi di associazione

In AWS Security Hub CSPM, un'associazione di criteri di configurazione potrebbe fallire per i seguenti motivi comuni.

- L'account di gestione Organizations non è un membro: se desideri associare una policy di configurazione all'account di gestione Organizations, tale account deve già avere AWS Security Hub CSPM abilitato. Questo rende l'account di gestione un account membro dell'organizzazione.
- AWS Confignon è abilitato o configurato correttamente: per abilitare gli standard in una politica di configurazione, AWS Config deve essere abilitato e configurato per registrare le risorse pertinenti.
- Deve essere associata da un account amministratore delegato: puoi associare una policy agli account di destinazione e alle unità organizzative solo quando hai effettuato l'accesso all'account amministratore CSPM di Security Hub delegato.
- È necessario associare una politica agli account e alle unità organizzative di destinazione solo dopo aver effettuato l'accesso alla propria regione d'origine.
- Opt-in Regione non abilitata: l'associazione delle politiche non riesce per un account membro o un'unità organizzativa in una regione collegata se si tratta di una regione con consenso esplicito che l'amministratore delegato non ha abilitato. È possibile riprovare dopo aver abilitato la regione dall'account amministratore delegato.
- Account membro sospeso: l'associazione delle politiche fallisce se si tenta di associare una politica a un account membro sospeso.

Aggiornamento delle politiche di configurazione

Dopo aver creato una politica di configurazione, l'account amministratore CSPM AWS di Security Hub delegato può aggiornare i dettagli e le associazioni delle politiche. Quando i dettagli della politica vengono aggiornati, gli account associati alla politica di configurazione iniziano automaticamente a utilizzare la politica aggiornata.

Per informazioni di base sui vantaggi della configurazione centralizzata e su come funziona, consultaComprendere la configurazione centrale in Security Hub CSPM.

> **Note**
>
> Le policy di configurazione supportano solo AWS standard e controlli. Non è possibile includere standard multicloud (come CIS Azure Foundations Benchmark v4.0.0) o controlli di Azure in una policy di configurazione. Inclusi un ARN standard multicloud o restituzioni di ID di controllo. `InvalidInputException` Per abilitare o configurare gli standard multicloud, utilizza i meccanismi di configurazione locali direttamente nell'area desiderata. Account AWS

L'amministratore delegato può aggiornare le seguenti impostazioni dei criteri:

- Abilita o disabilita Security Hub CSPM.
- Abilita uno o più standard di sicurezza.
- Indica quali controlli di sicurezza sono abilitati negli standard abilitati. È possibile farlo fornendo un elenco di controlli specifici che devono essere abilitati e Security Hub CSPM disabilita tutti gli altri controlli, inclusi i nuovi controlli quando vengono rilasciati. In alternativa, puoi fornire un elenco di controlli specifici che devono essere disabilitati e Security Hub CSPM abilita tutti gli altri controlli, inclusi i nuovi controlli quando vengono rilasciati.
- Facoltativamente, personalizza i parametri per selezionare i controlli abilitati tra gli standard abilitati.

Scegli il tuo metodo preferito e segui i passaggi per aggiornare una politica di configurazione.

> **Note**
>
> Se si utilizza la configurazione centrale, Security Hub CSPM disattiva automaticamente i controlli che coinvolgono risorse globali in tutte le regioni tranne la regione di origine. Gli altri

controlli che scegli di abilitare tramite una politica di configurazione sono abilitati in tutte le regioni in cui sono disponibili. Per limitare i risultati di questi controlli a una sola regione, puoi aggiornare le impostazioni del AWS Config registratore e disattivare la registrazione globale delle risorse in tutte le regioni tranne la regione d'origine.
Se un controllo abilitato che coinvolge risorse globali non è supportato nella regione di origine, Security Hub CSPM tenta di abilitare il controllo in una regione collegata in cui il controllo è supportato. Con la configurazione centralizzata, ti manca la copertura per un controllo che non è disponibile nella regione d'origine o in nessuna delle regioni collegate. Per un elenco dei controlli che coinvolgono risorse globali, consultaControlli che utilizzano risorse globali.

Console

Per aggiornare le politiche di configurazione

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore CSPM di Security Hub delegato nella regione di residenza.
2. Nel riquadro di navigazione, scegli Impostazioni e configurazione.
3. Scegliere la scheda Policy.
4. Seleziona la politica di configurazione che desideri modificare e scegli Modifica. Se lo desideri, modifica le impostazioni dei criteri. Lasciate questa sezione così com'è se desiderate mantenere invariate le impostazioni dei criteri.
5. Scegliete Avanti. Se lo desiderate, modificate le associazioni di policy. Lasciate questa sezione così com'è se desiderate mantenere invariate le associazioni di politiche. È possibile associare o dissociare la policy a un massimo di 15 destinazioni (account, unità organizzative o root) quando la si aggiorna.
6. Scegli Next (Successivo).
7. Controlla le modifiche e scegli Salva e applica. Nella tua regione d'origine e nelle regioni collegate, questa azione sostituisce le impostazioni di configurazione esistenti degli account associati a questa politica di configurazione. Gli account possono essere associati a una politica di configurazione tramite l'applicazione o ereditati da un nodo principale.

API

Per aggiornare le politiche di configurazione

1. Per aggiornare le impostazioni in una politica di configurazione, richiama l'UpdateConfigurationPolicyAPI dall'account amministratore delegato CSPM di Security Hub nella regione di residenza.
2. Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione che desideri aggiornare.
3. Fornisci valori aggiornati per i campi `ConfigurationPolicy` sottostanti. Facoltativamente, puoi anche fornire un motivo per l'aggiornamento.
4. Per aggiungere nuove associazioni per questa politica di configurazione, richiama l'StartConfigurationPolicyAssociationAPI dall'account amministratore delegato CSPM di Security Hub nella regione di residenza. Per rimuovere una o più associazioni correnti, richiama l'StartConfigurationPolicyDisassociationAPI dall'account amministratore delegato CSPM di Security Hub nella regione di origine.
5. Per il `ConfigurationPolicyIdentifier` campo, fornisci l'ARN o l'ID della politica di configurazione di cui desideri aggiornare le associazioni.
6. Per il `Target` campo, fornite gli account, le unità organizzative o l'ID root che desiderate associare o dissociare. Questa azione sostituisce le precedenti associazioni di policy per le unità organizzative o gli account specificati.

> **Note**
>
> Quando si richiama l'`UpdateConfigurationPolicy`API, Security Hub CSPM esegue una sostituzione completa dell'elenco per i campi`EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers`, e. `SecurityControlCustomParameters` Ogni volta che richiami questa API, fornisci l'elenco completo degli standard che desideri abilitare e l'elenco completo dei controlli che desideri abilitare o disabilitare e per cui personalizzare i parametri.

Esempio di richiesta API per aggiornare una politica di configurazione:

```
{
```

```
    "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

Per aggiornare le politiche di configurazione

1. Per aggiornare le impostazioni in una politica di configurazione, esegui il update-configuration-policycomando dall'account amministratore delegato CSPM di Security Hub nella regione di residenza.
2. Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione che desideri aggiornare.
3. Fornisci valori aggiornati per i campi `configuration-policy` sottostanti. Facoltativamente, puoi anche fornire un motivo per l'aggiornamento.
4. Per aggiungere nuove associazioni per questa politica di configurazione, esegui il start-configuration-policy-associationcomando dall'account amministratore delegato CSPM di Security Hub nell'area di residenza. Per rimuovere una o più associazioni correnti, esegui il start-configuration-policy-disassociationcomando dall'account amministratore delegato CSPM di Security Hub nella regione di origine.
5. Per il `configuration-policy-identifier` campo, fornisci l'ARN o l'ID della politica di configurazione di cui desideri aggiornare le associazioni.
6. Per il `target` campo, fornite gli account, le unità organizzative o l'ID root che desiderate associare o dissociare. Questa azione sostituisce le precedenti associazioni di policy per le unità organizzative o gli account specificati.

> **Note**
>
> Quando si esegue il `update-configuration-policy` comando, Security Hub CSPM esegue una sostituzione completa dell'elenco per i `EnabledStandardIdentifiers` campi, `EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers`, `eSecurityControlCustomParameters`. Ogni volta che esegui questo comando, fornisci l'elenco completo degli standard che desideri abilitare e l'elenco completo dei controlli per cui desideri abilitare o disabilitare e personalizzare i parametri.

Comando di esempio per aggiornare una politica di configurazione:

```
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}}}}]}}}'
```

L'`StartConfigurationPolicyAssociation`API restituisce un campo chiamato`AssociationStatus`. Questo campo indica se un'associazione di politiche è in sospeso o in uno stato di successo o di fallimento. La modifica dello stato da a `SUCCESS` o `FAILURE` può richiedere fino a 24 ore. `PENDING` Per ulteriori informazioni sullo stato dell'associazione, vedereRevisione dello stato di associazione di una politica di configurazione.

Eliminazione dei criteri di configurazione

Dopo aver creato una politica di configurazione, l'amministratore CSPM AWS di Security Hub delegato può eliminarla. In alternativa, l'amministratore delegato può mantenere la politica, ma dissociarla da account o unità organizzative (OU) specifici o dalla radice. Per istruzioni sulla dissociazione di una politica, vedere. Dissociazione di una configurazione dai suoi obiettivi

Per informazioni di base sui vantaggi della configurazione centralizzata e su come funziona, consulta. Comprendere la configurazione centrale in Security Hub CSPM

Questa sezione spiega come eliminare i criteri di configurazione.

Quando si elimina una politica di configurazione, questa non esiste più per l'organizzazione. Gli account di destinazione, le unità organizzative e la radice dell'organizzazione non possono più utilizzare la politica di configurazione. Le destinazioni associate a una politica di configurazione eliminata ereditano la politica di configurazione del genitore più vicino o vengono gestite automaticamente se il genitore più vicino è autogestito. Se si desidera che una destinazione utilizzi una configurazione diversa, è possibile associare la destinazione a una nuova politica di configurazione. Per ulteriori informazioni, consulta Creazione e associazione di policy di configurazione.

Ti consigliamo di creare e associare almeno una politica di configurazione alla tua organizzazione per fornire una copertura di sicurezza adeguata.

Prima di poter eliminare una politica di configurazione, è necessario dissociarla da qualsiasi account, unità organizzativa o radice a cui si applica attualmente.

Scegliete il metodo preferito e seguite i passaggi per eliminare una politica di configurazione.

Console

Come eliminare una policy di configurazione

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore CSPM di Security Hub delegato nella regione di residenza.
2. Nel pannello di navigazione, scegli Impostazioni e configurazione.
3. Scegliere la scheda Policy. Seleziona la politica di configurazione che desideri eliminare e scegli Elimina. Se la politica di configurazione è ancora associata a qualsiasi account o unità organizzativa, ti viene richiesto di dissociare la politica da tali destinazioni prima di poterla eliminare.
4. Controlla il messaggio di conferma. Inserisci **`confirm`** e scegli Elimina.

API

Come eliminare una policy di configurazione

Richiama l'DeleteConfigurationPolicyAPI dall'account amministratore delegato CSPM di Security Hub nella regione di origine.

Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione che desideri eliminare. Se ricevi un `ConflictException` errore, la politica di configurazione si applica ancora agli account o alle unità organizzative della tua organizzazione. Per risolvere l'errore, dissocia la politica di configurazione da questi account o unità organizzative prima di provare a eliminarla.

Esempio di richiesta API per eliminare una politica di configurazione:

```
{
```

```
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Come eliminare una policy di configurazione

Esegui il delete-configuration-policycomando dall'account amministratore delegato CSPM di Security Hub nella regione di origine.

Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione che desideri eliminare. Se ricevi un `ConflictException` errore, la politica di configurazione si applica ancora agli account o alle unità organizzative della tua organizzazione. Per risolvere l'errore, dissocia la politica di configurazione da questi account o unità organizzative prima di provare a eliminarla.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Dissociazione di una configurazione dai suoi obiettivi

Dall'account amministratore delegato AWS di Security Hub CSPM, è possibile dissociare una politica di configurazione o una configurazione autogestita da un account, un'unità organizzativa o una radice. La disassociazione mantiene la politica per usi futuri, ma rimuove le associazioni esistenti da account, unità organizzative o root specifici. È possibile dissociare solo una configurazione applicata direttamente, non una configurazione ereditata. Per modificare una configurazione ereditata, è possibile applicare una politica di configurazione o un comportamento autogestito all'account o all'unità organizzativa interessati. È inoltre possibile applicare una nuova politica di configurazione, che include le modifiche desiderate, al genitore più vicino.

La disassociazione non elimina una politica di configurazione. La politica viene mantenuta nel tuo account, quindi puoi associarla ad altri obiettivi della tua organizzazione. Per istruzioni sull'eliminazione di una politica di configurazione, consulta. Eliminazione dei criteri di configurazione Una volta completata la dissociazione, l'obiettivo interessato eredita la politica di configurazione o il comportamento autogestito del genitore più vicino. Se non esiste una configurazione ereditabile,

una destinazione mantiene le impostazioni che aveva prima della disassociazione ma viene gestita automaticamente.

Scegli il metodo preferito e segui i passaggi per dissociare un account, un'unità organizzativa o un utente root dalla configurazione corrente.

Console

Per dissociare un account o un'unità organizzativa dalla configurazione corrente

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore CSPM di Security Hub delegato nella regione di residenza.
2. Nel riquadro di navigazione, scegli Impostazioni e configurazione.
3. Nella scheda Organizations, seleziona l'account, l'unità organizzativa o la radice che desideri dissociare dalla configurazione corrente. Scegli Modifica.
4. Nella pagina Definisci configurazione, per Gestione, scegli Politica applicata se desideri che l'amministratore delegato sia in grado di applicare le politiche direttamente alla destinazione. Scegli Inherited se desideri che la destinazione erediti la configurazione del suo elemento principale più vicino. In entrambi i casi, l'amministratore delegato controlla le impostazioni per la destinazione. Scegli Self-managedse desideri che l'account o l'unità organizzativa controllino le proprie impostazioni.
5. Dopo aver esaminato le modifiche, scegli Avanti e Applica. Questa azione sostituisce le configurazioni esistenti di tutti gli account o le unità organizzative che rientrano nell'ambito, se tali configurazioni sono in conflitto con le selezioni correnti.

API

Per dissociare un account o un'unità organizzativa dalla configurazione corrente

1. Richiama l'StartConfigurationPolicyDisassociationAPI dall'account amministratore delegato CSPM di Security Hub nella regione di origine.
2. Per`ConfigurationPolicyIdentifier`, fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione da cui desideri dissociare. Inserisci questo campo `SELF_MANAGED_SECURITY_HUB` per dissociare il comportamento autogestito.

3. Per`Target`, fornisci gli account, le unità organizzative o la directory principale che desideri separare da questa politica di configurazione.

Esempio di richiesta API per dissociare una politica di configurazione:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Per dissociare un account o un'unità organizzativa dalla configurazione corrente

1. Esegui il start-configuration-policy-disassociationcomando dall'account amministratore delegato CSPM di Security Hub nella regione di origine.
2. Per`configuration-policy-identifier`, fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione da cui desideri dissociare. Inserisci questo campo `SELF_MANAGED_SECURITY_HUB` per dissociare il comportamento autogestito.
3. Per`target`, fornisci gli account, le unità organizzative o la directory principale che desideri separare da questa politica di configurazione.

Esempio di comando per dissociare una politica di configurazione:

```
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"}'
```

Configurazione di uno standard o di un controllo nel contesto

Quando si utilizza la configurazione centrale in AWS Security Hub CSPM, l'amministratore delegato di Security Hub CSPM può creare politiche di configurazione che specificano in che modo Security Hub CSPM, gli standard di sicurezza e i controlli di sicurezza sono configurati per un'organizzazione.

L'amministratore delegato può associare le politiche a account e unità organizzative (OU) specifici. Le politiche hanno effetto nella regione di origine e in tutte le regioni collegate. L'amministratore delegato può aggiornare le politiche di configurazione se necessario.

Nella console Security Hub CSPM, l'amministratore delegato può aggiornare i criteri di configurazione in due modi: dalla pagina Configurazione o nel contesto dei flussi di lavoro esistenti. Quest'ultima opzione può essere utile perché, man mano che si visualizzano i risultati di sicurezza, è possibile scoprire quali standard e controlli sono più pertinenti per il proprio ambiente e configurarli allo stesso tempo.

In-context la configurazione è disponibile solo sulla console Security Hub CSPM. A livello di codice, l'amministratore delegato deve richiamare il UpdateConfigurationPolicyfunzionamento dell'API CSPM Security Hub per modificare il modo in cui gli standard o i controlli specifici sono configurati nell'organizzazione.

Segui questi passaggi per configurare uno standard o un controllo CSPM di Security Hub nel contesto.

Per configurare uno standard o un controllo nel contesto (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore CSPM di Security Hub delegato nella regione di residenza.
2. Nel riquadro di navigazione, scegli una delle seguenti opzioni:

   - Per configurare uno standard, scegli Standard di sicurezza e scegli uno standard specifico.
   - Per configurare un controllo, scegli Controlli e scegli un controllo specifico.
3. La console elenca le politiche di configurazione CSPM di Security Hub esistenti e lo stato dello standard o del controllo selezionato in ciascuna di esse. Scegli le opzioni per abilitare o disabilitare lo standard o il controllo in ogni politica di configurazione esistente. Per quanto riguarda i controlli, puoi anche scegliere di personalizzare i parametri di controllo. Non è possibile creare una nuova politica durante la configurazione contestuale. Per creare una nuova politica, devi andare alla pagina Configurazione, scegliere la scheda Politiche, quindi scegliere Crea politica.
4. Dopo aver apportato le modifiche, scegli Avanti.

5. Controlla le modifiche e scegli Applica. Gli aggiornamenti riguardano tutti gli account e le unità organizzative associati a una politica di configurazione modificata. Gli aggiornamenti hanno effetto anche nella regione di origine e in tutte le regioni collegate.

Disabilitazione della configurazione centrale in Security Hub CSPM

Quando si disabilita la configurazione centrale in AWS Security Hub CSPM, l'amministratore delegato perde la possibilità di configurare Security Hub CSPM, gli standard di sicurezza e i controlli di sicurezza su più Account AWS unità organizzative (OU) e. Regioni AWS È invece necessario configurare la maggior parte delle impostazioni separatamente per ogni account in ogni regione.

> **Important**
>
> Prima di poter disattivare la configurazione centrale, è necessario dissociare gli account e le unità organizzative dalla configurazione corrente, che si tratti di una politica di configurazione o di un comportamento autogestito.
> Prima di poter disabilitare la configurazione centrale, è necessario eliminare anche le politiche di configurazione esistenti.

Quando si disabilita la configurazione centrale, si verificano le seguenti modifiche:

- L'amministratore delegato non può più creare politiche di configurazione per l'organizzazione.
- Gli account a cui era stata applicata o ereditata una politica di configurazione mantengono le impostazioni correnti, ma si gestiscono automaticamente.
- L'organizzazione passa alla configurazione locale. Nella configurazione locale, la maggior parte delle impostazioni CSPM di Security Hub deve essere configurata separatamente in ogni account e regione dell'organizzazione. L'amministratore delegato può scegliere di abilitare automaticamente Security Hub CSPM, gli standard di sicurezza predefiniti e tutti i controlli che fanno parte degli standard predefiniti nei nuovi account dell'organizzazione. Gli standard predefiniti sono AWS Foundational Security Best Practices (FSBP) e Center for Internet Security (CIS) Foundations Benchmark v1.2.0. AWS Queste impostazioni hanno effetto solo nella regione corrente e influiscono solo sui nuovi account dell'organizzazione. L'amministratore delegato non può modificare gli standard predefiniti. La configurazione locale non supporta l'uso di politiche di configurazione o la configurazione a livello di unità organizzativa.

L'identità dell'account amministratore delegato rimane la stessa quando si smette di utilizzare la configurazione centrale. Anche la regione d'origine e le regioni collegate rimangono invariate (la regione d'origine è ora denominata regione di aggregazione e può essere utilizzata per trovare aggregazioni).

Scegli il tuo metodo preferito e segui i passaggi per smettere di usare la configurazione centrale e passare alla configurazione locale.

Security Hub CSPM console

Per disabilitare la configurazione centrale (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore CSPM di Security Hub delegato nella regione di residenza.
2. Nel pannello di navigazione, scegli Impostazioni e configurazione.
3. Nella sezione Panoramica, scegli Modifica.
4. Nella casella Modifica configurazione dell'organizzazione, scegli Configurazione locale. Se non l'hai già fatto, ti viene richiesto di annullare l'associazione ed eliminare le politiche di configurazione correnti prima di poter interrompere la configurazione centrale. Gli account o le unità organizzative designati come autogestiti devono essere dissociati dalla relativa configurazione autogestita. È possibile eseguire questa operazione nella console modificando il tipo di gestione di ogni account o unità organizzativa autogestito in Gestito centralmente e eredita dalla mia organizzazione.
5. Facoltativamente, selezionare le impostazioni predefinite di configurazione locale per i nuovi account dell'organizzazione.
6. Scegli Conferma.

Security Hub CSPM API

Per disabilitare la configurazione centrale (API)

1. Invoca l'UpdateOrganizationConfigurationAPI.
2. Imposta il `ConfigurationType` campo nell'`OrganizationConfiguration`oggetto su. `LOCAL` L'API restituisce un errore se sono presenti politiche di configurazione o

associazioni di politiche esistenti. Per dissociare una politica di configurazione, richiama l'`StartConfigurationPolicyDisassociation`API. Per eliminare una politica di configurazione, richiama l'API. `DeleteConfigurationPolicy`

3. Se desideri abilitare automaticamente Security Hub CSPM nei nuovi account dell'organizzazione, imposta il `AutoEnable` campo su. `true` Per impostazione predefinita, il valore di questo campo è `false` e Security Hub CSPM non viene abilitato automaticamente nei nuovi account dell'organizzazione. Facoltativamente, se desideri abilitare automaticamente gli standard di sicurezza predefiniti nei nuovi account dell'organizzazione, imposta il `AutoEnableStandards` campo su. `DEFAULT` Questo è il valore predefinito. Se non desideri abilitare automaticamente gli standard di sicurezza predefiniti nei nuovi account dell'organizzazione, imposta il `AutoEnableStandards` campo su`NONE`.

Esempio di richiesta API:

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

Per disabilitare la configurazione centrale (AWS CLI)

1. Esegui il comando update-organization-configuration.
2. Imposta il `ConfigurationType` campo nell'`organization-configuration`oggetto su`LOCAL`. Il comando restituisce un errore se sono presenti criteri di configurazione o associazioni di criteri esistenti. Per dissociare una politica di configurazione, esegui il `start-configuration-policy-disassociation` comando. Per eliminare una politica di configurazione, esegui il `delete-configuration-policy` comando.
3. Se desideri abilitare automaticamente Security Hub CSPM nei nuovi account dell'organizzazione, includi il `auto-enable` parametro. Per impostazione predefinita, il valore di questo parametro è `no-auto-enable` e Security Hub CSPM non viene abilitato automaticamente nei nuovi account dell'organizzazione. Facoltativamente, se

desideri abilitare automaticamente gli standard di sicurezza predefiniti nei nuovi account dell'organizzazione, imposta il `auto-enable-standards` campo su. `DEFAULT` Questo è il valore predefinito. Se non desideri abilitare automaticamente gli standard di sicurezza predefiniti nei nuovi account dell'organizzazione, imposta il `auto-enable-standards` campo su`NONE`.

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Gestione degli account di amministratore e membro in Security Hub CSPM

Se il tuo AWS ambiente ha più account, puoi trattare gli account che utilizzano AWS Security Hub CSPM come account membro e associarli a un singolo account amministratore. L'amministratore può monitorare il livello di sicurezza generale dell'utente e intraprendere le azioni consentite sugli account dei membri. L'amministratore può anche eseguire diverse attività di gestione e amministrazione degli account su larga scala, come il monitoraggio dei costi di utilizzo stimati e la valutazione delle quote degli account.

È possibile associare gli account dei membri a un amministratore in due modi: integrando Security Hub CSPM AWS Organizations o inviando e accettando manualmente gli inviti di iscrizione in Security Hub CSPM.

Gestione degli account conAWS Organizations

AWS Organizationsè un servizio globale di gestione degli account che consente AWS agli amministratori di consolidare e gestire più account. Account AWS Fornisce funzionalità di gestione degli account e fatturazione consolidata progettate per supportare le esigenze di budget, sicurezza e conformità. È offerto senza costi aggiuntivi e si integra con più sistemiServizi AWS, tra cui AWS Security Hub CSPM, Amazon Macie e Amazon. GuardDuty Per ulteriori informazioni, consulta la Guida per l'utente AWS Organizations.

Quando si integra Security Hub CSPM eAWS Organizations, l'account di gestione Organizations designa un amministratore delegato CSPM di Security Hub. Security Hub CSPM viene abilitato automaticamente nell'account amministratore delegato Regione AWS in cui è stato designato.

Dopo aver designato un amministratore delegato, consigliamo di gestire gli account in Security Hub CSPM con configurazione centrale. Questo è il modo più efficiente per personalizzare Security Hub CSPM e garantire un'adeguata copertura di sicurezza per l'organizzazione.

La configurazione centrale consente all'amministratore delegato di personalizzare Security Hub CSPM su più account e regioni dell'organizzazione anziché eseguire la configurazione. Region-by-Region È possibile creare una politica di configurazione per l'intera organizzazione o creare politiche di configurazione diverse per account e unità organizzative diversi. Le politiche specificano se Security Hub CSPM è abilitato o disabilitato negli account associati e quali standard e controlli di sicurezza sono abilitati.

L'amministratore delegato può designare gli account come gestiti centralmente o autogestiti. Gli account gestiti centralmente sono configurabili solo dall'amministratore delegato. Self-managed gli account possono specificare le proprie impostazioni.

Se non si attiva la configurazione centrale, l'amministratore delegato ha una capacità più limitata di configurare Security Hub CSPM, chiamata configurazione locale. Nella configurazione locale, l'amministratore delegato può abilitare automaticamente Security Hub CSPM e gli standard di sicurezza predefiniti nei nuovi account dell'organizzazione nella regione corrente. Tuttavia, gli account esistenti non utilizzano queste impostazioni, quindi è possibile che si verifichi una variazione della configurazione dopo che un account si unisce all'organizzazione.

Oltre a queste nuove impostazioni dell'account, la configurazione locale è specifica dell'account e. Region-specific Ogni account dell'organizzazione deve configurare il servizio, gli standard e i controlli CSPM di Security Hub separatamente in ciascuna regione. La configurazione locale, inoltre, non supporta l'uso di policy di configurazione.

Gestione manuale degli account tramite invito

È necessario gestire manualmente gli account dei membri su invito in Security Hub CSPM se si dispone di un account autonomo o se non si integra con Organizations. Un account autonomo non può integrarsi con Organizations, quindi è necessario gestirlo manualmente. Ti consigliamo di integrare AWS Organizations e utilizzare la configurazione centrale se aggiungerai altri account in futuro.

Quando si utilizza la gestione manuale degli account, si designa un account come amministratore CSPM di Security Hub. L'account amministratore può visualizzare i dati negli account dei membri e intraprendere determinate azioni in base ai risultati degli account dei membri. L'amministratore

CSPM di Security Hub invita altri account a diventare account membro e la relazione amministratore-membro viene stabilita quando un potenziale account membro accetta l'invito.

La gestione manuale degli account non supporta l'uso di politiche di configurazione. Senza policy di configurazione, l'amministratore non può personalizzare centralmente Security Hub CSPM configurando impostazioni variabili per account diversi. Invece, ogni account dell'organizzazione deve abilitare e configurare Security Hub CSPM separatamente in ciascuna regione. Ciò può rendere più difficile e dispendioso in termini di tempo garantire un'adeguata copertura di sicurezza in tutti gli account e le regioni in cui si utilizza Security Hub CSPM. Ciò può anche causare variazioni nella configurazione, in quanto gli account membri possono specificare le proprie impostazioni senza alcun intervento da parte dell'amministratore.

Per gestire gli account su invito, consultaGestione degli account tramite invito in Security Hub CSPM.

Consigli per la gestione di più account in Security Hub CSPM

La sezione seguente riassume alcune restrizioni e raccomandazioni da tenere a mente quando si gestiscono gli account dei membri in AWS Security Hub CSPM.

Numero massimo di account membri

Se si utilizza l'integrazione conAWS Organizations, Security Hub CSPM supporta fino a 10.000 account membro per account amministratore delegato in ciascuno. Regione AWS Se abiliti e gestisci Security Hub CSPM manualmente, Security Hub CSPM supporta fino a 1.000 inviti di account membro per account amministratore in ciascuna regione.

Creazione di relazioni amministratore-membro

> **Note**
>
> Se utilizzi l'integrazione CSPM di Security Hub con AWS Organizations e non hai invitato manualmente alcun account membro, questa sezione non ti riguarda.

Un account non può essere contemporaneamente un account amministratore e un account membro.

Un account membro può essere associato a un solo account amministratore. Se un account dell'organizzazione è abilitato dall'account amministratore CSPM di Security Hub, l'account non può accettare un invito da un altro account. Se un account ha già accettato un invito, l'account non può

essere abilitato dall'account amministratore CSPM di Security Hub per l'organizzazione. Inoltre, non può ricevere inviti da altri account.

Per la procedura di invito manuale, l'accettazione di un invito all'iscrizione è facoltativa.

Iscrizione tramiteAWS Organizations

Se si integra Security Hub CSPM conAWS Organizations, l'account di gestione Organizations può designare un account amministratore delegato (DA) per Security Hub CSPM. L'account di gestione dell'organizzazione non può essere impostato come DA in Organizations. Sebbene ciò sia consentito in Security Hub CSPM, consigliamo che l'account di gestione Organizations non sia il DA.

Ti consigliamo di scegliere lo stesso account DA in tutte le regioni. Se utilizzi la configurazione centrale, Security Hub CSPM imposta lo stesso account DA in tutte le regioni in cui configuri Security Hub CSPM per la tua organizzazione.

Ti consigliamo inoltre di scegliere lo stesso account DA per tutti i servizi di AWS sicurezza e conformità per aiutarti a gestire i problemi relativi alla sicurezza in un unico pannello di controllo.

Iscrizione su invito

Per gli account membro creati su invito, l'associazione tra account amministratore e membro viene creata solo nella regione da cui viene inviato l'invito. L'account amministratore deve abilitare Security Hub CSPM in ogni regione in cui si desidera utilizzarlo. L'account amministratore invita quindi ogni account a diventare un account membro in quella regione.

> **Note**
>
> Ti consigliamo di utilizzare AWS Organizations al posto degli inviti CSPM di Security Hub per gestire gli account dei membri.

Coordinamento degli account di amministratore tra i vari servizi

Security Hub CSPM aggrega i risultati di vari AWS servizi, come Amazon, Amazon GuardDuty Inspector e Amazon Macie. Security Hub CSPM consente inoltre agli utenti di passare da un GuardDuty risultato all'avvio di un'indagine in Amazon Detective.

Tuttavia, le relazioni amministratore-membro impostate in questi altri servizi non si applicano automaticamente a Security Hub CSPM. Security Hub CSPM consiglia di utilizzare lo stesso account

dell'account amministratore per tutti questi servizi. Questo account amministratore deve essere un account responsabile degli strumenti di sicurezza. Lo stesso account deve essere utilizzato anche come account aggregatore perAWS Config.

Ad esempio, un utente dell'account GuardDuty amministratore A può visualizzare i risultati GuardDuty degli account membro B e C sulla GuardDuty console. Se l'account A abilita quindi Security Hub CSPM, gli utenti dell'account A non visualizzano automaticamente GuardDuty i risultati per gli account B e C nel CSPM di Security Hub. Per questi account è inoltre richiesta una relazione amministratore-membro del Security Hub CSPM.

A tale scopo, imposta l'account A come account amministratore CSPM di Security Hub e abilita gli account B e C a diventare account membri CSPM di Security Hub.

Gestione del Security Hub CSPM per più account conAWS Organizations

È possibile integrare AWS Security Hub CSPM e quindi gestire Security Hub CSPM per gli account dell'organizzazione. AWS Organizations

Per integrare Security Hub CSPM conAWS Organizations, devi creare un'organizzazione in. AWS Organizations L'account di gestione Organizations designa un account come amministratore delegato CSPM di Security Hub per l'organizzazione. L'amministratore delegato può quindi abilitare Security Hub CSPM per altri account dell'organizzazione, aggiungere tali account come account membro CSPM di Security Hub e intraprendere le azioni consentite sugli account dei membri. L'amministratore delegato CSPM di Security Hub può abilitare e gestire Security Hub CSPM per un massimo di 10.000 account membri.

L'estensione delle capacità di configurazione dell'amministratore delegato dipende dall'utilizzo o meno della configurazione centrale. Con la configurazione centrale abilitata, non è necessario configurare Security Hub CSPM separatamente in ogni account membro e. Regione AWS L'amministratore delegato può applicare impostazioni CSPM specifiche di Security Hub in account membri e unità organizzative (OU) specifici in tutte le regioni.

L'account amministratore delegato CSPM di Security Hub può eseguire le seguenti azioni sugli account dei membri:

- Se utilizzi la configurazione centrale, configura centralmente Security Hub CSPM per gli account dei membri e le unità organizzative creando politiche di configurazione CSPM di Security Hub. Le policy di configurazione possono essere utilizzate per abilitare e disabilitare Security Hub CSPM, abilitare e disabilitare gli standard e abilitare e disabilitare i controlli.

- Tratta automaticamente i nuovi account come account membri del Security Hub CSPM quando entrano a far parte dell'organizzazione. Se si utilizza la configurazione centrale, una politica di configurazione associata a un'unità organizzativa include account nuovi e esistenti che fanno parte dell'unità organizzativa.
- Tratta gli account dell'organizzazione esistenti come account membri del Security Hub CSPM. Ciò avviene automaticamente se si utilizza la configurazione centrale.
- Dissocia gli account dei membri che appartengono all'organizzazione. Se si utilizza la configurazione centrale, è possibile dissociare un account membro solo dopo averlo designato come autogestito. In alternativa, è possibile associare una politica di configurazione che disabiliti Security Hub CSPM a specifici account membro gestiti centralmente.

Se non si attiva la configurazione centralizzata, l'organizzazione utilizza il tipo di configurazione predefinito chiamato configurazione locale. Nella configurazione locale, l'amministratore delegato ha una capacità più limitata di applicare le impostazioni negli account dei membri. Per ulteriori informazioni, consulta Comprendere la configurazione locale in Security Hub CSPM.

Per un elenco completo delle azioni che l'amministratore delegato può eseguire sugli account dei membri, vedere. Azioni consentite dagli account amministratore e membro in Security Hub CSPM

Gli argomenti di questa sezione spiegano come integrare Security Hub CSPM AWS Organizations e come gestire Security Hub CSPM per gli account di un'organizzazione. Ove pertinente, ogni sezione identifica i vantaggi e le differenze di gestione per gli utenti della configurazione centrale.

Argomenti

- Integrazione del Security Hub CSPM conAWS Organizations
- Abilitazione automatica di Security Hub CSPM nei nuovi account dell'organizzazione
- Abilitazione manuale di Security Hub CSPM nei nuovi account dell'organizzazione
- Dissociazione degli account dei membri di Security Hub CSPM dall'organizzazione

Integrazione del Security Hub CSPM conAWS Organizations

Per integrare AWS Security Hub CSPM eAWS Organizations, è necessario creare un'organizzazione in Organizations e utilizzare l'account di gestione dell'organizzazione per designare un account amministratore CSPM di Security Hub delegato. Ciò consente a Security Hub CSPM come servizio affidabile in Organizations. Abilita inoltre Security Hub CSPM nella versione corrente Regione AWS per l'account amministratore delegato e consente all'amministratore delegato di abilitare Security

Hub CSPM per gli account membro, visualizzare i dati negli account membro ed eseguire altre azioni consentite sugli account dei membri.

Se si utilizza la configurazione centrale, l'amministratore delegato può anche creare politiche di configurazione CSPM di Security Hub che specificano come il servizio, gli standard e i controlli CSPM di Security Hub devono essere configurati negli account dell'organizzazione.

Creazione di un'organizzazione

Un'organizzazione è un'entità creata per consolidare la propria in Account AWS modo da poterla amministrare come una singola unità.

Puoi creare un'organizzazione utilizzando la AWS Organizations console o utilizzando un comando proveniente da AWS CLI o da una delle API SDK. Per istruzioni dettagliate, consulta Creare un'organizzazione nella Guida per l'AWS Organizationsutente.

Puoi utilizzarlo AWS Organizations per visualizzare e gestire centralmente tutti gli account all'interno della tua organizzazione. Un'organizzazione ha un account di gestione insieme a zero o più account membri. È possibile organizzare gli account in una struttura gerarchica ad albero con una radice nella parte superiore e unità organizzative (OU) annidate sotto la radice. Ogni account può trovarsi direttamente sotto la radice o collocato in una delle unità organizzative della gerarchia. Un'unità organizzativa è un contenitore per account specifici. Ad esempio, è possibile creare un'unità organizzativa finanziaria che includa tutti i conti relativi alle operazioni finanziarie.

Consigli per la scelta dell'amministratore CSPM delegato di Security Hub

Se disponi di un account amministratore dopo la procedura di invito manuale e stai passando alla gestione dell'account conAWS Organizations, ti consigliamo di designare quell'account come amministratore delegato del Security Hub CSPM.

Sebbene le API e la console CSPM di Security Hub consentano all'account di gestione dell'organizzazione di essere l'amministratore delegato di Security Hub CSPM, consigliamo di scegliere due account diversi. Questo perché è probabile che gli utenti che hanno accesso all'account di gestione dell'organizzazione per gestire la fatturazione siano diversi dagli utenti che devono accedere al CSPM di Security Hub per la gestione della sicurezza.

Si consiglia di utilizzare lo stesso amministratore delegato in tutte le regioni. Se opti per la configurazione centralizzata, Security Hub CSPM designa automaticamente lo stesso amministratore delegato nella tua regione di origine e in tutte le regioni collegate.

Verifica le autorizzazioni per configurare l'amministratore delegato

Per designare e rimuovere un account amministratore CSPM di Security Hub delegato, l'account di gestione dell'organizzazione deve disporre delle autorizzazioni per le azioni e `EnableOrganizationAdminAccount` in `DisableOrganizationAdminAccount` Security Hub CSPM. L'account di gestione Organizations deve inoltre disporre delle autorizzazioni amministrative per Organizations.

Per concedere tutte le autorizzazioni richieste, collega le seguenti politiche gestite da Security Hub CSPM al principale IAM per l'account di gestione dell'organizzazione:

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

Designazione dell'amministratore delegato

Per designare l'account amministratore CSPM di Security Hub delegato, è possibile utilizzare la console CSPM di Security Hub, l'API CSPM di Security Hub oppure. AWS CLI Security Hub CSPM imposta l'amministratore delegato Regione AWS solo nella versione corrente ed è necessario ripetere l'azione in altre regioni. Se inizi a utilizzare la configurazione centrale, Security Hub CSPM imposta automaticamente lo stesso amministratore delegato nella regione di origine e nelle regioni collegate.

L'account di gestione dell'organizzazione non deve abilitare Security Hub CSPM per designare l'account amministratore CSPM di Security Hub delegato.

È consigliabile che l'account di gestione dell'organizzazione non sia l'account amministratore delegato di Security Hub CSPM. Tuttavia, se si sceglie l'account di gestione dell'organizzazione come amministratore delegato CSPM di Security Hub, l'account di gestione deve avere il CSPM di Security Hub abilitato. Se l'account di gestione non ha Security Hub CSPM abilitato, è necessario abilitare il CSPM di Security Hub manualmente. Security Hub CSPM non può essere abilitato automaticamente per l'account di gestione dell'organizzazione.

È necessario designare l'amministratore CSPM delegato di Security Hub utilizzando uno dei seguenti metodi. La designazione dell'amministratore delegato di Security Hub CSPM con le API Organizations non si riflette in Security Hub CSPM.

Scegli il tuo metodo preferito e segui i passaggi per designare l'account amministratore CSPM di Security Hub delegato.

Security Hub CSPM console

Per designare l'amministratore delegato durante l'onboarding

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Scegli Vai a Security Hub CSPM. Ti viene richiesto di accedere all'account di gestione dell'organizzazione.
3. Nella pagina Designa amministratore delegato, nella sezione Account amministratore delegato, specifica l'account amministratore delegato. Ti consigliamo di scegliere lo stesso amministratore delegato che hai impostato per altri AWS servizi di sicurezza e conformità.
4. Scegli Imposta amministratore delegato. Ti viene richiesto di accedere all'account amministratore delegato (se non lo sei già) per continuare l'onboarding con la configurazione centrale. Se non desideri avviare la configurazione centralizzata, scegli Annulla. L'amministratore delegato è impostato, ma non stai ancora utilizzando la configurazione centrale.

Per designare l'amministratore delegato dal Settings page

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel pannello di navigazione CSPM di Security Hub, scegli Impostazioni. Quindi scegli Generale.
3. Se al momento è assegnato un account amministratore CSPM di Security Hub, prima di poter designare un nuovo account, è necessario rimuovere l'account corrente.

   In Amministratore delegato, per rimuovere l'account corrente, scegli Rimuovi.
4. Inserisci l'ID dell'account che desideri designare come account amministratore CSPM di Security Hub.

   È necessario designare lo stesso account amministratore CSPM di Security Hub in tutte le regioni. Se si designa un account diverso da quello designato in altre regioni, la console restituisce un errore.
5. Scegli Delega.

Security Hub CSPM API,AWS CLI

Dall'account di gestione dell'organizzazione, utilizza il EnableOrganizationAdminAccountfunzionamento dell'API CSPM Security Hub. Se utilizzi ilAWS CLI, esegui il comando. enable-organization-admin-account Fornisci l'Account AWSID dell'amministratore CSPM di Security Hub delegato.

L'esempio seguente designa l'amministratore CSPM delegato di Security Hub. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

Rimozione o modifica dell'amministratore delegato

Solo l'account di gestione dell'organizzazione può rimuovere l'account amministratore CSPM di Security Hub delegato.

Per cambiare l'amministratore delegato di Security Hub CSPM, è necessario prima rimuovere l'account amministratore delegato corrente e quindi designarne uno nuovo.

> **Warning**
>
> Quando si utilizza la configurazione centrale, non è possibile utilizzare la console CSPM di Security Hub o le API CSPM di Security Hub per modificare o rimuovere l'account amministratore delegato. Se l'account di gestione dell'organizzazione utilizza la AWS Organizations console o le AWS Organizations API per modificare o rimuovere l'amministratore delegato di Security Hub CSPM, Security Hub CSPM interrompe automaticamente la configurazione centrale ed elimina i criteri di configurazione e le associazioni di policy. Gli account dei membri mantengono le configurazioni che avevano prima della modifica o della rimozione dell'amministratore delegato.

Se si utilizza la console Security Hub CSPM per rimuovere l'amministratore delegato in una regione, l'amministratore delegato viene rimosso automaticamente in tutte le regioni.

L'API CSPM di Security Hub rimuove solo l'account amministratore CSPM di Security Hub delegato dalla regione in cui viene emessa la chiamata o il comando API. È necessario ripetere l'azione in altre regioni.

Se si utilizza l'API Organizations per rimuovere l'account amministratore CSPM delegato di Security Hub, questo viene rimosso automaticamente in tutte le regioni.

Rimozione dell'amministratore delegato (Organizations API,AWS CLI)

È possibile utilizzare Organizations per rimuovere l'amministratore CSPM delegato di Security Hub in tutte le regioni.

Se si utilizza la configurazione centrale per gestire gli account, la rimozione dell'account amministratore delegato comporta l'eliminazione delle politiche di configurazione e delle associazioni di politiche. Gli account membro mantengono le configurazioni che avevano prima della modifica o della rimozione dell'amministratore delegato. Tuttavia, questi account non possono più essere gestiti dall'account amministratore delegato rimosso. Diventano account autogestiti che devono essere configurati separatamente in ciascuna regione.

Scegli il tuo metodo preferito e segui le istruzioni per rimuovere l'account amministratore CSPM di Security Hub delegato con. AWS Organizations

Organizations API,AWS CLI

Per rimuovere l'amministratore CSPM delegato di Security Hub

Dall'account di gestione dell'organizzazione, utilizza il DeregisterDelegatedAdministratorfunzionamento dell'API Organizations. Se utilizzi ilAWS CLI, esegui il comando deregister-delegated-administrator. Fornisci l'ID account dell'amministratore delegato e il responsabile del servizio per Security Hub CSPM, che è. `securityhub.amazonaws.com`

L'esempio seguente rimuove l'amministratore CSPM delegato di Security Hub. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

Rimozione dell'amministratore delegato (console Security Hub CSPM)

È possibile utilizzare la console CSPM di Security Hub per rimuovere l'amministratore CSPM di Security Hub delegato in tutte le regioni.

Quando l'account amministratore delegato di Security Hub CSPM viene rimosso, gli account membro vengono dissociati dall'account amministratore CSPM di Security Hub delegato rimosso.

Il CSPM di Security Hub è ancora abilitato negli account dei membri. Diventano account autonomi finché un nuovo amministratore CSPM di Security Hub non li abilita come account membro.

Se l'account di gestione dell'organizzazione non è un account abilitato in Security Hub CSPM, utilizza l'opzione nella pagina CSPM di benvenuto in Security Hub.

Per rimuovere l'account amministratore CSPM di Security Hub delegato dal Benvenuto in Security Hub CSPM page

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Scegli Vai a Security Hub.
3. In Amministratore delegato, scegli Rimuovi.

Se l'account di gestione dell'organizzazione è un account abilitato in Security Hub, utilizza l'opzione nella scheda Generale della pagina Impostazioni.

Per rimuovere l'account amministratore CSPM di Security Hub delegato dal Settings page

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel pannello di navigazione CSPM di Security Hub, scegli Impostazioni. Quindi scegli Generale.
3. In Amministratore delegato, scegli Rimuovi.

Rimozione dell'amministratore delegato (Security Hub, API CSPM),AWS CLI)

È possibile utilizzare l'API CSPM di Security Hub o le operazioni CSPM di Security Hub per rimuovere l'amministratore CSPM AWS CLI delegato di Security Hub. Quando si rimuove l'amministratore delegato con uno di questi metodi, questo viene rimosso solo nella regione in cui è stata emessa la chiamata o il comando API. Security Hub CSPM non aggiorna altre regioni e non rimuove l'account amministratore delegato in. AWS Organizations

Scegli il tuo metodo preferito e segui questi passaggi per rimuovere l'account amministratore delegato di Security Hub CSPM con Security Hub CSPM.

Security Hub CSPM API,AWS CLI

Per rimuovere l'amministratore CSPM delegato di Security Hub

Dall'account di gestione dell'organizzazione, utilizza il DisableOrganizationAdminAccountfunzionamento dell'API CSPM Security Hub. Se utilizzi ilAWS CLI, esegui il comando. disable-organization-admin-account Fornisci l'ID account dell'amministratore CSPM di Security Hub delegato.

L'esempio seguente rimuove l'amministratore CSPM delegato di Security Hub. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Disattivazione dell'integrazione CSPM di Security Hub conAWS Organizations

Dopo l'integrazione di un'AWS Organizationsorganizzazione con AWS Security Hub CSPM, l'account di gestione Organizations può successivamente disabilitare l'integrazione. Come utente dell'account di gestione Organizations, puoi farlo disabilitando l'accesso affidabile per Security Hub CSPM in. AWS Organizations

Quando si disabilita l'accesso affidabile per Security Hub CSPM, si verifica quanto segue:

- Security Hub CSPM perde lo status di servizio affidabile in. AWS Organizations
- L'account amministratore delegato CSPM di Security Hub perde l'accesso alle impostazioni, ai dati e alle risorse CSPM di Security Hub per tutti gli account membri CSPM di Security Hub. Regioni AWS
- Se stavi utilizzando la configurazione centrale, Security Hub CSPM smette automaticamente di utilizzarla per la tua organizzazione. Le policy di configurazione e le associazioni di policy vengono eliminate. Gli account mantengono le configurazioni che avevano prima della disattivazione dell'accesso affidabile.
- Tutti gli account membri di Security Hub CSPM diventano account autonomi e mantengono le impostazioni correnti. Se Security Hub CSPM è stato abilitato per un account membro in una o più regioni, Security Hub CSPM continua a essere abilitato per l'account in tali regioni. Anche gli standard e i controlli abilitati rimangono invariati. Puoi modificare queste impostazioni separatamente in ogni account e regione. Tuttavia, l'account non è più associato a un amministratore delegato in nessuna regione.

Per ulteriori informazioni sui risultati della disabilitazione dell'accesso affidabile ai servizi, vedere Using AWS Organizations with other Servizi AWS nella Guida per l'AWS Organizationsutente.

Per disabilitare l'accesso affidabile, puoi utilizzare la AWS Organizations console, l'API Organizations oAWS CLI. Solo un utente dell'account di gestione Organizations può disabilitare l'accesso affidabile ai servizi per Security Hub CSPM. Per i dettagli sulle autorizzazioni necessarie, consulta Autorizzazioni necessarie per disabilitare l'accesso affidabile nella Guida per l'utente. AWS Organizations

Prima di disabilitare l'accesso affidabile, consigliamo di collaborare con l'amministratore delegato dell'organizzazione per disabilitare Security Hub CSPM negli account dei membri e per ripulire le risorse CSPM di Security Hub in tali account.

Scegli il tuo metodo preferito e segui i passaggi per disabilitare l'accesso affidabile per Security Hub CSPM.

Organizations console

Per disabilitare l'accesso affidabile per Security Hub CSPM

1. Accedi Console di gestione AWS utilizzando le credenziali dell'account di gestione. AWS Organizations
2. Apri la console Organizations all'indirizzo https://console.aws.amazon.com/organizations/.
3. Nel riquadro di navigazione, scegli Servizi.
4. In Servizi integrati, scegli AWSSecurity Hub CSPM.
5. Scegli Disable trusted access (Disabilita accesso attendibile).
6. Conferma di voler disabilitare l'accesso affidabile.

Organizations API

Per disabilitare l'accesso affidabile per Security Hub CSPM

Richiama il DisableAWSServiceAccessfunzionamento dell'API. AWS Organizations Per il `ServicePrincipal` parametro, specificare il principale del servizio CSPM di Security Hub ()`securityhub.amazonaws.com`.

AWS CLI

Per disabilitare l'accesso affidabile per Security Hub CSPM

Esegui il comando disable-aws-service-access dell'API. AWS Organizations Per il `service-principal` parametro, specificare il principale del servizio CSPM di Security Hub ()`securityhub.amazonaws.com`.

Esempio:

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

Abilitazione automatica di Security Hub CSPM nei nuovi account dell'organizzazione

Quando nuovi account entrano a far parte dell'organizzazione, vengono aggiunti all'elenco nella pagina Account della console CSPM di AWS Security Hub. Per gli account dell'organizzazione, Tipo è Per organizzazione. Per impostazione predefinita, i nuovi account non diventano membri del Security Hub CSPM quando entrano a far parte dell'organizzazione. Il loro stato è Non membro. L'account amministratore delegato può aggiungere automaticamente nuovi account come membri e abilitare Security Hub CSPM in questi account quando entrano a far parte dell'organizzazione.

> **Note**
>
> Sebbene molti Regioni AWS siano attivi per impostazione predefinita per l'utenteAccount AWS, è necessario attivare alcune regioni manualmente. In questo documento, queste regioni sono chiamate regioni opt-in. Per abilitare automaticamente Security Hub CSPM in un nuovo account in una regione opt-in, l'account deve prima avere quella regione attivata. Solo il proprietario dell'account può attivare la regione di attivazione. Per ulteriori informazioni sulle regioni che richiedono l'iscrizione, vedi Specificare quali possono essere utilizzate dal Regioni AWS tuo account.

Questo processo è diverso a seconda che si utilizzi la configurazione centrale (consigliata) o la configurazione locale.

Abilitazione automatica di nuovi account aziendali (configurazione centrale)

Se si utilizza la configurazione centrale, è possibile abilitare automaticamente Security Hub CSPM negli account dell'organizzazione nuovi ed esistenti creando una politica di configurazione in cui sia abilitato Security Hub CSPM. È quindi possibile associare la politica alla radice dell'organizzazione o alle unità organizzative (OU) specifiche.

Se si associa una politica di configurazione in cui Security Hub CSPM è abilitato a un'unità organizzativa specifica, Security Hub CSPM viene automaticamente abilitato in tutti gli account (esistenti e nuovi) che appartengono a quell'unità organizzativa. I nuovi account che non appartengono all'unità organizzativa vengono gestiti automaticamente e non hanno automaticamente il Security Hub CSPM abilitato. Se si associa una politica di configurazione in cui Security Hub CSPM è abilitato alla radice, Security Hub CSPM viene automaticamente abilitato in tutti gli account (esistenti e nuovi) che entrano a far parte dell'organizzazione. Le eccezioni si verificano se un account utilizza una politica diversa tramite l'applicazione o l'ereditarietà o è autogestito.

Nella politica di configurazione, è inoltre possibile definire quali standard e controlli di sicurezza devono essere abilitati nell'unità organizzativa. Per generare risultati di controllo per gli standard abilitati, gli account nell'unità organizzativa devono essere AWS Config abilitati e configurati per registrare le risorse richieste. Per ulteriori informazioni sulla AWS Config registrazione, vedere Attivazione e configurazione AWS Config.

Per istruzioni sulla creazione di una politica di configurazione, vedereCreazione e associazione di policy di configurazione.

Abilitazione automatica di nuovi account aziendali (configurazione locale)

Quando si utilizza la configurazione locale e si attiva l'abilitazione automatica degli standard predefiniti, Security Hub CSPM aggiunge nuovi account dell'organizzazione come membri e abilita Security Hub CSPM in essi nella regione corrente. Le altre regioni non sono interessate. Inoltre, l'attivazione dell'abilitazione automatica non abilita Security Hub CSPM negli account aziendali esistenti, a meno che non siano già stati aggiunti come account membro.

Dopo aver attivato l'abilitazione automatica, gli standard di sicurezza predefiniti vengono abilitati per i nuovi account membro nella regione corrente quando entrano a far parte dell'organizzazione. Gli standard predefiniti sono AWS Foundational Security Best Practices (FSBP) e Center for Internet Security (CIS) Foundations Benchmark v1.2.0. AWS Non è possibile modificare gli standard predefiniti. Se desideri abilitare altri standard in tutta l'organizzazione o abilitare gli standard per determinati account e unità organizzative, ti consigliamo di utilizzare la configurazione centrale.

Per generare risultati di controllo per gli standard predefiniti (e altri standard abilitati), gli account dell'organizzazione devono essere AWS Config abilitati e configurati per registrare le risorse richieste. Per ulteriori informazioni sulla AWS Config registrazione, vedere Attivazione e configurazione AWS Config.

Scegli il tuo metodo preferito e segui i passaggi per abilitare automaticamente Security Hub CSPM nei nuovi account dell'organizzazione. Queste istruzioni si applicano solo se si utilizza la configurazione locale.

Security Hub CSPM console

Per abilitare automaticamente i nuovi account dell'organizzazione come membri CSPM di Security Hub

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Sign utilizza le credenziali dell'account amministratore delegato.
2. Nel pannello di navigazione CSPM di Security Hub, in Impostazioni, scegli Configurazione.
3. Nella sezione Account, attiva gli account. Auto-enable

Security Hub CSPM API

Per abilitare automaticamente i nuovi account dell'organizzazione come membri CSPM di Security Hub

Richiama l'`UpdateOrganizationConfiguration`API dall'account amministratore delegato. Imposta il `AutoEnable` campo su per `true` abilitare automaticamente Security Hub CSPM nei nuovi account dell'organizzazione.

AWS CLI

Per abilitare automaticamente i nuovi account dell'organizzazione come membri CSPM di Security Hub

Esegui il `update-organization-configuration`comando dall'account amministratore delegato. Includi il `auto-enable` parametro per abilitare automaticamente Security Hub CSPM nei nuovi account dell'organizzazione.

```
aws securityhub update-organization-configuration --auto-enable
```

Abilitazione manuale di Security Hub CSPM nei nuovi account dell'organizzazione

Se non abiliti automaticamente Security Hub CSPM nei nuovi account dell'organizzazione quando entrano a far parte dell'organizzazione, puoi aggiungere tali account come membri e abilitare il CSPM di Security Hub manualmente dopo l'adesione all'organizzazione. È inoltre necessario abilitare manualmente Security Hub CSPM in quanto in precedenza Account AWS si è dissociati da un'organizzazione.

> **Note**
>
> Questa sezione non si applica all'utente se si utilizza la configurazione centrale. Se si utilizza la configurazione centrale, è possibile creare politiche di configurazione che abilitano Security Hub CSPM in account membri e unità organizzative (OU) specifici. È inoltre possibile abilitare standard e controlli specifici in tali account e unità organizzative.

Non puoi abilitare Security Hub CSPM in un account se è già un account membro di un'altra organizzazione.

Inoltre, non puoi abilitare Security Hub CSPM in un account attualmente sospeso. Se tenti di abilitare il servizio in un account sospeso, lo stato dell'account cambia in Account sospeso.

- Se l'account non ha Security Hub CSPM abilitato, Security Hub CSPM è abilitato in quell'account. Nell'account sono abilitati anche lo standard AWS Foundational Security Best Practices (FSBP) e CIS AWS Foundations Benchmark v1.2.0, a meno che non si disattivino gli standard di sicurezza predefiniti.

  L'eccezione è l'account di gestione Organizations. Security Hub CSPM non può essere abilitato automaticamente nell'account di gestione Organizations. È necessario abilitare manualmente Security Hub CSPM nell'account di gestione Organizations prima di poterlo aggiungere come account membro.
- Se l'account ha già abilitato Security Hub CSPM, Security Hub CSPM non apporta altre modifiche all'account. Abilita solo l'iscrizione.

Affinché Security Hub CSPM generi i risultati del controllo, gli account dei membri devono essere AWS Config abilitati e configurati per registrare le risorse richieste. Per ulteriori informazioni, consulta Abilitazione e configurazione di AWS Config.

Scegli il tuo metodo preferito e segui i passaggi per abilitare un account dell'organizzazione come account membro CSPM di Security Hub.

Security Hub CSPM console

Per abilitare manualmente gli account dell'organizzazione come membri CSPM di Security Hub

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore delegato.
2. Nel pannello di navigazione CSPM di Security Hub, in Impostazioni, scegli Configurazione.
3. Nell'elenco Account, seleziona ogni account dell'organizzazione che desideri abilitare.
4. Scegli Azioni, quindi scegli Aggiungi membro.

Security Hub CSPM API

Per abilitare manualmente gli account dell'organizzazione come membri CSPM di Security Hub

Richiama l'`CreateMembers`API dall'account amministratore delegato. Per ogni account da abilitare, fornisci l'ID dell'account.

A differenza della procedura di invito manuale, quando `CreateMembers` richiami per abilitare un account dell'organizzazione, non devi inviare un invito.

AWS CLI

Per abilitare manualmente gli account dell'organizzazione come membri CSPM di Security Hub

Esegui il `create-members`comando dall'account amministratore delegato. Per ogni account da abilitare, fornisci l'ID dell'account.

A differenza della procedura di invito manuale, quando `create-members` esegui l'attivazione di un account aziendale, non devi inviare un invito.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Esempio

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Dissociazione degli account dei membri di Security Hub CSPM dall'organizzazione

Per interrompere la ricezione e la visualizzazione dei risultati da un account membro CSPM di AWS Security Hub, puoi dissociare l'account membro dalla tua organizzazione.

> **Note**
>
> Se si utilizza la configurazione centrale, la dissociazione funziona in modo diverso. È possibile creare una politica di configurazione che disabiliti Security Hub CSPM in uno o più account membro gestiti centralmente. Dopodiché, questi account fanno ancora parte dell'organizzazione, ma non genereranno risultati CSPM di Security Hub. Se utilizzi la configurazione centrale ma disponi anche di account membri invitati manualmente, puoi dissociare uno o più account invitati manualmente.

Gli account membro gestiti utilizzando non AWS Organizations possono dissociare i propri account dall'account amministratore. Solo l'account amministratore può dissociare un account membro.

La dissociazione di un account membro non comporta la chiusura dell'account. Rimuove invece l'account membro dall'organizzazione. L'account membro dissociato diventa autonomo Account AWS e non è più gestito dall'integrazione CSPM di Security Hub con. AWS Organizations

Scegli il tuo metodo preferito e segui i passaggi per dissociare un account membro dall'organizzazione.

Security Hub CSPM console

Per dissociare un account membro dall'organizzazione

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore delegato.
2. Nel riquadro di navigazione, in Impostazioni, scegli Configurazione.
3. Nella sezione Account, seleziona gli account da cui desideri dissociare. Se utilizzi la configurazione centrale, puoi selezionare un account invitato manualmente da dissociare dalla scheda. `Invitation accounts` Questa scheda è visibile solo se si utilizza la configurazione centrale.
4. Scegli Azioni, quindi scegli Dissocia account.

Security Hub CSPM API

Per dissociare un account membro dall'organizzazione

Richiama l'`DisassociateMembers`API dall'account amministratore delegato. È necessario fornire Account AWS gli ID per la dissociazione degli account dei membri. Per visualizzare un elenco di account membri, richiama l'`ListMembers`API.

AWS CLI

Per dissociare un account membro dall'organizzazione

Esegui il `disassociate-members` comando > dall'account amministratore delegato. È necessario fornire Account AWS gli ID per la dissociazione degli account dei membri. Per visualizzare un elenco di account membri, esegui il `list-members` comando >.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Esempio

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Puoi anche utilizzare la AWS Organizations console o gli AWS CLI AWS SDK per dissociare un account membro dalla tua organizzazione. Per ulteriori informazioni, consulta Rimuovere un account membro dalla propria organizzazione nella Guida per l'AWS Organizationsutente.

Gestione degli account tramite invito in Security Hub CSPM

È possibile gestire centralmente più account CSPM di AWS Security Hub in due modi: integrando Security Hub CSPM AWS Organizations o inviando e accettando manualmente gli inviti di iscrizione. È necessario utilizzare la procedura manuale se si dispone di un account autonomo o se non si esegue l'integrazione con. AWS Organizations Nella gestione manuale degli account, l'amministratore CSPM di Security Hub invita gli account a diventare membri. La relazione amministratore-membro viene stabilita quando un potenziale membro accetta l'invito. Un account amministratore CSPM di Security Hub può gestire Security Hub CSPM per un massimo di 1.000 account membro basati su invito.

> **Note**
>
> Se crei un'organizzazione basata su inviti in Security Hub CSPM, puoi successivamente passare a usare invece. AWS Organizations Se hai più di un account membro, ti consigliamo di utilizzare AWS Organizations al posto degli inviti CSPM di Security Hub per gestire i tuoi account membro. Per informazioni, consulta Gestione del Security Hub CSPM per più account conAWS Organizations.

Cross-Region l'aggregazione dei risultati e di altri dati è disponibile per gli account che inviti tramite la procedura di invito manuale. Tuttavia, l'amministratore deve invitare l'account membro della regione di aggregazione e di tutte le regioni collegate affinché l'aggregazione tra regioni funzioni. Inoltre, l'account membro deve avere il Security Hub CSPM abilitato nella regione di aggregazione e in tutte le regioni collegate per consentire all'amministratore di visualizzare i risultati dell'account membro.

Le politiche di configurazione non sono supportate per gli account membro invitati manualmente. È invece necessario configurare le impostazioni CSPM di Security Hub separatamente in ogni account membro e Regione AWS quando si utilizza la procedura di invito manuale.

È inoltre necessario utilizzare la procedura manuale basata sugli inviti per gli account che non appartengono alla propria organizzazione. Ad esempio, potresti non includere un account di prova nella tua organizzazione. In alternativa, potresti voler consolidare gli account di più organizzazioni in un unico account amministratore CSPM di Security Hub. L'account amministratore CSPM di Security Hub deve inviare inviti agli account che appartengono ad altre organizzazioni.

Nella pagina Configurazione della console CSPM di Security Hub, gli account aggiunti su invito sono elencati nella scheda Account di invito. Se utilizzi la configurazione centrale, ma inviti anche account esterni all'organizzazione, puoi visualizzare i risultati degli account basati su invito in questa scheda. Tuttavia, l'amministratore CSPM di Security Hub non può configurare account basati su inviti in tutte le regioni tramite l'uso di politiche di configurazione.

Gli argomenti di questa sezione spiegano come gestire gli account dei membri tramite gli inviti.

Argomenti

- Aggiungere e invitare account membri in Security Hub CSPM
- Rispondere a un invito a diventare un account membro CSPM di Security Hub
- Dissociazione degli account dei membri in Security Hub CSPM
- Eliminazione degli account dei membri in Security Hub CSPM

- Dissociazione da un account amministratore CSPM di Security Hub
- Passaggio a Organizations per gestire gli account in Security Hub CSPM

Aggiungere e invitare account membri in Security Hub CSPM

> **Note**
>
> Ti consigliamo di utilizzare AWS Organizations al posto degli inviti CSPM di Security Hub per gestire gli account dei membri. Per informazioni, consulta Gestione del Security Hub CSPM per più account conAWS Organizations.

Il tuo account diventa l'amministratore CSPM AWS di Security Hub per gli account che accettano il tuo invito a diventare un account membro CSPM di Security Hub.

Quando accetti un invito da un altro account, il tuo account diventa un account membro e quell'account diventa il tuo amministratore.

Se il tuo account è un account amministratore, non puoi accettare un invito a diventare un account membro.

L'aggiunta di un account membro prevede i seguenti passaggi:

1. L'account amministratore aggiunge l'account membro al relativo elenco di account membri.
2. L'account amministratore invia un invito all'account membro.
3. L'account membro accetta l'invito.

Aggiungere account membri

Dalla console CSPM di Security Hub, puoi aggiungere account all'elenco degli account membri. Nella console Security Hub CSPM, è possibile selezionare gli account singolarmente o caricare un `.csv` file contenente le informazioni sull'account.

Per ogni account, è necessario fornire l'ID dell'account e un indirizzo e-mail. L'indirizzo e-mail deve essere l'indirizzo e-mail da contattare in merito ai problemi di sicurezza dell'account. Non viene utilizzato per verificare l'account.

Scegli il tuo metodo preferito e segui i passaggi per aggiungere account membri.

Security Hub CSPM console

Per aggiungere account al tuo elenco di account membri

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore.
2. Nel riquadro a sinistra, scegliere Settings (Impostazioni).
3. Nella pagina Impostazioni, scegli Account, quindi scegli Aggiungi account. Puoi quindi aggiungere account singolarmente o caricare un `.csv` file contenente l'elenco degli account.
4. Per selezionare gli account, esegui una delle seguenti operazioni:

   - Per aggiungere gli account singolarmente, in Inserisci account, inserisci l'ID account e l'indirizzo e-mail dell'account da aggiungere, quindi scegli Aggiungi.

     Ripeti questa procedura per ogni account.
   - Per utilizzare un file con valori separati da virgole (.csv) per aggiungere più account, devi prima creare il file. Il file deve contenere l'ID dell'account e l'indirizzo e-mail di ogni account da aggiungere.

     Nell'`.csv`elenco, gli account devono apparire uno per riga. La prima riga del `.csv` file deve contenere l'intestazione. Nell'intestazione, la prima colonna è **`Account ID`** e la seconda colonna è. **`Email`**

     Ogni riga successiva deve contenere un ID account e un indirizzo e-mail validi per l'account da aggiungere.

     Ecco un esempio di `.csv` file visualizzato in un editor di testo.

     ```
     Account ID,Email
     111111111111,user@example.com
     ```

     In un programma per fogli di calcolo, i campi vengono visualizzati in colonne separate. Il formato sottostante è ancora separato da virgole. È necessario formattare gli ID degli account come numeri non decimali. Ad esempio, l'ID account 444455556666 non può essere formattato come 444455556666.0. Assicurati inoltre che la formattazione del numero non rimuova gli zeri iniziali dall'ID dell'account.

Per selezionare il file, sulla console, scegli Carica lista (.csv). Quindi scegli Sfoglia.

Dopo aver selezionato il file, scegli Aggiungi account.

5. Dopo aver aggiunto gli account, in Account da aggiungere, scegli Avanti.

Security Hub CSPM API

Per aggiungere account al tuo elenco di account membri

Richiama l'`CreateMembers`API dall'account amministratore. Per aggiungere un account membro, devi fornire l'Account AWSID.

AWS CLI

Per aggiungere account al tuo elenco di account membri

Esegui il `create-members`comando dall'account amministratore. Per ogni account membro da aggiungere, devi fornire l'Account AWSID.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Esempio

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Invitare gli account dei membri

Dopo aver aggiunto gli account membro, invii un invito all'account membro. Puoi anche inviare nuovamente un invito a un account che hai dissociato dall'amministratore.

Security Hub CSPM console

Per invitare account di potenziali membri

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore.
2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli Account.

3. Per l'account da invitare, scegliere Invite (Invita) nella colonna Status (Stato).
4. Quando ti viene richiesto di confermare, scegli Invita.

> **Note**
>
> Per inviare nuovamente gli inviti ad account dissociati, seleziona ciascun account dissociato nella pagina Account. Per Azioni, scegli Reinvia l'invito.

Security Hub CSPM API

Per invitare account di potenziali membri

Richiama l'`InviteMembers`API dall'account amministratore. Per ogni account da invitare, devi fornire l'Account AWSID.

AWS CLI

Per invitare account di potenziali membri

Esegui il `invite-members`comando dall'account amministratore. Per ogni account da invitare, devi fornire l'Account AWSID.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Esempio

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Rispondere a un invito a diventare un account membro CSPM di Security Hub

> **Note**
>
> Ti consigliamo di utilizzare AWS Organizations al posto degli inviti CSPM di Security Hub per gestire gli account dei membri. Per informazioni, consulta Gestione del Security Hub CSPM per più account conAWS Organizations.

Puoi accettare o rifiutare un invito a diventare un account membro CSPM AWS di Security Hub.

Se accetti un invito, il tuo account diventa un account membro del Security Hub CSPM. L'account che ha inviato l'invito diventa il tuo account amministratore CSPM di Security Hub. L'utente dell'account amministratore può visualizzare i risultati del proprio account membro in Security Hub CSPM.

Se rifiuti l'invito, il tuo account viene contrassegnato come Rinunciato nell'elenco degli account membri dell'account amministratore.

Puoi accettare solo un invito a diventare un account membro.

Prima di poter accettare o rifiutare un invito, è necessario abilitare Security Hub CSPM.

Ricorda che tutti gli account CSPM di Security Hub devono essere AWS Config abilitati e configurati per registrare tutte le risorse. Per i dettagli sui requisiti perAWS Config, vedere Attivazione e configurazione. AWS Config

Accettazione di un invito

È possibile inviare un invito a diventare un account membro CSPM di Security Hub dall'account amministratore. È quindi possibile accettare l'invito dopo aver effettuato l'accesso all'account membro.

Scegli il tuo metodo preferito e segui i passaggi per accettare un invito a diventare un account membro.

Security Hub CSPM console

Per accettare un invito all'iscrizione

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli Account.
3. Nella sezione Account amministratore, attiva Accetta, quindi scegli Accetta invito.

Security Hub CSPM API

Per accettare un invito all'iscrizione

Richiama l'`AcceptAdministratorInvitation`API. È necessario fornire l'identificatore dell'invito e l'Account AWSID dell'account amministratore. Per recuperare i dettagli sull'invito, usa l'`ListInvitations`operazione.

AWS CLI

Per accettare un invito all'iscrizione

Esegui il comando `accept-administrator-invitation`. È necessario fornire l'identificatore dell'invito e l'Account AWSID dell'account amministratore. Per recuperare i dettagli sull'invito, esegui il `list-invitations`comando.

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

Esempio

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> La console CSPM di Security Hub continua a essere utilizzata. `AcceptInvitation` Alla fine cambierà modalità di utilizzo. `AcceptAdministratorInvitation` Tutte le policy IAM che controllano specificamente l'accesso a questa funzione devono continuare a essere utilizzate`AcceptInvitation`. È inoltre necessario `AcceptAdministratorInvitation` completare le policy per garantire che siano disponibili le autorizzazioni corrette dopo l'inizio dell'utilizzo `AcceptAdministratorInvitation` della console.

Rifiutare un invito

Puoi rifiutare un invito a diventare un account membro CSPM di Security Hub. Quando rifiuti un invito nella console CSPM di Security Hub, il tuo account viene contrassegnato come Rinunciato nell'elenco degli account membri dell'account amministratore. Lo stato Dimesso viene visualizzato solo quando si accede alla console CSPM di Security Hub utilizzando l'account amministratore. Tuttavia, l'invito rimane invariato nella console dell'account membro finché non si accede all'account amministratore e si elimina l'invito.

Per rifiutare un invito, devi accedere all'account membro che ha ricevuto l'invito.

Scegli il tuo metodo preferito e segui i passaggi per rifiutare un invito a diventare un account membro.

Security Hub CSPM console

Per rifiutare un invito all'iscrizione

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli Account.
3. Nella sezione Account amministratore, scegli Rifiuta l'invito.

Security Hub CSPM API

Per rifiutare un invito all'iscrizione

Richiama l'`DeclineInvitations`API. È necessario fornire l'Account AWSID dell'account amministratore che ha emesso l'invito. Per visualizzare le informazioni sugli inviti, utilizza l'`ListInvitations`operazione.

AWS CLI

Per rifiutare un invito all'iscrizione

Esegui il comando `decline-invitations`. È necessario fornire l'Account AWSID dell'account amministratore che ha emesso l'invito. Per visualizzare le informazioni sugli inviti, esegui il `list-invitations`comando.

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Esempio

```
aws securityhub decline-invitations --account-ids "123456789012"
```

Dissociazione degli account dei membri in Security Hub CSPM

> **Note**
>
> Ti consigliamo di utilizzare AWS Organizations al posto degli inviti CSPM di Security Hub per gestire gli account dei membri. Per informazioni, consulta Gestione del Security Hub CSPM per più account conAWS Organizations.

Un account amministratore CSPM di AWS Security Hub può dissociare un account membro per interrompere la ricezione e la visualizzazione dei risultati da quell'account. È necessario dissociare un account membro prima di poterlo eliminare.

Quando dissociate un account membro, questo rimane nell'elenco degli account membri con lo stato Rimosso (Non associato). L'account viene rimosso dalle informazioni relative all'account amministratore dell'account membro.

Per riprendere a ricevere i risultati relativi all'account, puoi inviare nuovamente l'invito. Per rimuovere completamente l'account membro, puoi eliminare l'account membro.

Scegli il tuo metodo preferito e segui i passaggi per dissociare un account membro invitato manualmente dall'account amministratore.

Security Hub CSPM console

Per dissociare un account membro invitato manualmente

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore.
2. Nel riquadro di navigazione, in Impostazioni, scegli Configurazione.
3. Nella sezione Account, seleziona gli account da cui desideri dissociare.
4. Scegli Azioni, quindi scegli Dissocia account.

Security Hub CSPM API

Per dissociare un account membro invitato manualmente

Richiama l'`DisassociateMembers`API dall'account amministratore. È necessario fornire gli Account AWS ID degli account dei membri da cui si desidera dissociare. Per visualizzare un elenco di account membri, utilizza l'`ListMembers`operazione.

AWS CLI

Per dissociare un account membro invitato manualmente

Esegui il `disassociate-members`comando dall'account amministratore. È necessario fornire gli Account AWS ID degli account dei membri da cui si desidera dissociare. Per visualizzare un elenco di account membri, esegui il `list-members`comando.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Esempio

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Eliminazione degli account dei membri in Security Hub CSPM

> **Note**
>
> Ti consigliamo di utilizzare AWS Organizations al posto degli inviti CSPM di Security Hub per gestire gli account dei membri. Per informazioni, consulta Gestione del Security Hub CSPM per più account conAWS Organizations.

Come account amministratore CSPM di AWS Security Hub, puoi eliminare gli account dei membri che sono stati aggiunti su invito. Prima di poter eliminare un account abilitato, è necessario dissociarlo.

Quando si elimina un account membro, questo viene completamente rimosso dall'elenco. Per ripristinare l'iscrizione dell'account, devi aggiungerlo e invitarlo nuovamente come se fosse un account membro completamente nuovo.

Non puoi eliminare gli account che appartengono a un'organizzazione e che vengono gestiti utilizzando l'integrazione conAWS Organizations.

Scegli il tuo metodo preferito e segui i passaggi per eliminare gli account dei membri invitati manualmente.

Security Hub CSPM console

Per eliminare un account membro invitato manualmente

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando l'account amministratore.
2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli Configurazione.

3. Scegli la scheda Account di invito. Quindi, seleziona gli account da eliminare.
4. Scegli Azioni, quindi Elimina. Questa opzione è disponibile solo se hai dissociato l'account. È necessario dissociare un account membro prima che possa essere eliminato.

Security Hub CSPM API

Per eliminare un account membro invitato manualmente

Richiama l'`DeleteMembers`API dall'account amministratore. È necessario fornire gli Account AWS ID degli account dei membri che si desidera eliminare. Per recuperare l'elenco degli account membri, richiama l'`ListMembers`API.

AWS CLI

Per eliminare un account membro invitato manualmente

Esegui il `delete-members`comando dall'account amministratore. È necessario fornire gli Account AWS ID degli account membro che si desidera eliminare. Per recuperare l'elenco degli account membri, esegui il `list-members`comando.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Esempio

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Dissociazione da un account amministratore CSPM di Security Hub

> **Note**
>
> Ti consigliamo di utilizzare AWS Organizations al posto degli inviti CSPM di Security Hub per gestire gli account dei membri. Per informazioni, consulta Gestione del Security Hub CSPM per più account conAWS Organizations.

Se il tuo account è stato aggiunto come account membro CSPM di AWS Security Hub su invito, puoi dissociare l'account membro dall'account amministratore. Dopo aver dissociato un account membro, Security Hub CSPM non invia i risultati dall'account all'account amministratore.

Gli account membro gestiti utilizzando l'integrazione con non AWS Organizations possono dissociare i propri account dall'account amministratore. Solo l'amministratore delegato di Security Hub CSPM può dissociare gli account dei membri gestiti con Organizations.

Quando ci si dissocia dall'account amministratore, l'account rimane nell'elenco dei membri dell'account amministratore con lo stato di Dimesso. Tuttavia, l'account amministratore non riceve alcun risultato relativo al tuo account.

Dopo la dissociazione dall'account amministratore, l'invito a diventare membro rimane valido. Potrai accettare nuovamente l'invito in futuro.

Security Hub CSPM console

Per dissociarsi dal proprio account amministratore

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli Account.
3. Nella sezione Account amministratore, disattiva Accetta, quindi scegli Aggiorna.

Security Hub CSPM API

Per dissociarti dal tuo account amministratore

Richiama l'API. `DisassociateFromAdministratorAccount`

AWS CLI

Per dissociarsi dal proprio account amministratore

Esegui il comando `disassociate-from-administrator-account`.

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> La console CSPM di Security Hub continua a essere utilizzata. `DisassociateFromMasterAccount` Alla fine cambierà modalità di utilizzo. `DisassociateFromAdministratorAccount` Tutte le policy IAM che

controllano specificamente l'accesso a questa funzione devono continuare a essere utilizzate`DisassociateFromMasterAccount`. È inoltre necessario `DisassociateFromAdministratorAccount` completare le policy per garantire che siano disponibili le autorizzazioni corrette dopo l'inizio dell'utilizzo `DisassociateFromAdministratorAccount` della console.

Passaggio a Organizations per gestire gli account in Security Hub CSPM

Quando gestisci gli account manualmente in AWS Security Hub CSPM, devi invitare account membri potenziali e configurare ogni account membro separatamente in ciascuno di essi. Regione AWS

Integrando Security Hub CSPM eAWS Organizations, puoi eliminare la necessità di inviare inviti e ottenere un maggiore controllo sul modo in cui Security Hub CSPM è configurato e personalizzato nella tua organizzazione. Per questo motivo, ti consigliamo di utilizzare AWS Organizations al posto degli inviti CSPM di Security Hub per gestire gli account dei membri. Per informazioni, consulta Gestione del Security Hub CSPM per più account conAWS Organizations.

È possibile utilizzare un approccio combinato in cui si utilizza l'AWS Organizationsintegrazione, ma anche invitare manualmente account esterni all'organizzazione. Tuttavia, consigliamo di utilizzare esclusivamente l'integrazione Organizations. La configurazione centrale, una funzionalità che consente di gestire Security Hub CSPM su più account e regioni, è disponibile solo in caso di integrazione con Organizations.

Questa sezione spiega come passare dalla gestione manuale degli account basata su inviti alla gestione degli account con. AWS Organizations

Integrazione del Security Hub CSPM conAWS Organizations

Innanzitutto, è necessario integrare Security Hub CSPM e. AWS Organizations

È possibile integrare questi servizi completando i seguenti passaggi:

- Crea un'organizzazione inAWS Organizations. Per istruzioni, consulta Creare un'organizzazione nella Guida AWS Organizations per l'utente.
- Dall'account di gestione Organizations, designare un account amministratore delegato CSPM di Security Hub.

> **Note**
>
> L'account di gestione dell'organizzazione non può essere impostato come account DA.

Per istruzioni dettagliate, vedi Integrazione del Security Hub CSPM conAWS Organizations.

Completando i passaggi precedenti, concedi l'accesso affidabile per Security Hub CSPM in. AWS Organizations Ciò abilita anche Security Hub CSPM nella versione corrente Regione AWS per l'account amministratore delegato.

L'amministratore delegato può gestire l'organizzazione in Security Hub CSPM, principalmente aggiungendo gli account dell'organizzazione come account membri CSPM di Security Hub. L'amministratore può anche accedere a determinate impostazioni, dati e risorse CSPM di Security Hub per tali account.

Quando si passa alla gestione degli account utilizzando Organizations, gli account basati su invito non diventano automaticamente membri CSPM di Security Hub. Solo gli account che aggiungi alla nuova organizzazione possono diventare membri del Security Hub CSPM.

Dopo aver attivato l'integrazione, puoi gestire gli account con Organizations. Per informazioni, consulta Gestione del Security Hub CSPM per più account conAWS Organizations. La gestione degli account varia in base al tipo di configurazione dell'organizzazione.

Azioni consentite dagli account amministratore e membro in Security Hub CSPM

Gli account amministratore e membro hanno accesso alle azioni CSPM di AWS Security Hub riportate nelle tabelle seguenti. Nelle tabelle, i valori hanno i seguenti significati:

- Qualsiasi: l'account può eseguire l'azione per qualsiasi account membro sotto lo stesso amministratore.
- Corrente: l'account può eseguire l'azione solo per se stesso (l'account a cui hai attualmente effettuato l'accesso).
- Dash: indica che l'account non è in grado di eseguire l'azione.

Come indicato nelle tabelle, le azioni consentite variano in base all'integrazione AWS Organizations e al tipo di configurazione utilizzato dall'organizzazione. Per informazioni sulla differenza tra configurazione centrale e locale, vedereGestione degli account conAWS Organizations.

Security Hub CSPM non copia i risultati degli account dei membri nell'account amministratore. In Security Hub CSPM, tutti i risultati vengono inseriti in una regione specifica per un account specifico. In ogni regione, l'account amministratore può visualizzare e gestire i risultati per i propri account membro in quella regione.

Se si imposta una regione di aggregazione, l'account amministratore può visualizzare e gestire i risultati degli account membro provenienti dalle regioni collegate che vengono replicati nella regione di aggregazione. Per ulteriori informazioni sull'aggregazione tra regioni, vedere aggregazione. Cross-Region

Le tabelle seguenti specificano le autorizzazioni predefinite per gli account amministratore e membro. Puoi utilizzare policy IAM personalizzate per limitare ulteriormente l'accesso alle caratteristiche e alle funzioni del Security Hub CSPM. Per indicazioni ed esempi, consulta il post sul blog Aligning IAM policies to user personas for AWS Security Hub CSPM.

Azioni consentite se si effettua l'integrazione con Organizations e si utilizza la configurazione centrale

Gli account amministratore e membro possono accedere alle azioni CSPM di Security Hub come segue se si effettua l'integrazione con Organizations e si utilizza la configurazione centrale.

Azione	Account amministratore delegato Security Hub CSPM	Account membro gestito centralmente	Self-managed account membro
Creare e gestire le politiche di configurazione CSPM di Security Hub	Per account gestiti autonomamente e centralmente	–	–
Visualizza gli account dell'organizzazione	Qualsiasi	–	–
Account socio dissociato	Qualsiasi	–	–

Azione	Account amministratore delegato Security Hub CSPM	Account membro gestito centralmente	Self-managed account membro
Eliminare l'account del membro	Qualsiasi account non aziendale	–	–
Disattiva Security Hub CSPM	Per conti correnti e conti gestiti centralmente	–	Corrente (deve essere dissociato dall'account amministratore)
Visualizza i risultati e la cronologia delle scoperte	Qualsiasi	Attuali	Attuali
Aggiorna i risultati	Qualsiasi	Attuali	Attuali
Visualizza i risultati delle analisi	Qualsiasi	Attuali	Attuali
Visualizza i dettagli del controllo	Qualsiasi	Attuali	Attuali
Attiva o disattiva i risultati del controllo consolidato	Qualsiasi	–	–
Abilita e disabilita gli standard	Per conti correnti e conti gestiti centralmente	–	Attuali
Abilita e disabilita i controlli	Per conti correnti e conti gestiti centralmente	–	Attuali
Abilita e disabilita le integrazioni	Attuali	Attuali	Attuali

Azione	Account amministratore delegato Security Hub CSPM	Account membro gestito centralmente	Self-managed account membro
Configura l'aggregazione tra regioni	Qualsiasi	–	–
Seleziona la regione d'origine e le regioni collegate	Qualsiasi (è necessario interrompere e riavviare la configurazione centrale per modificare la regione di origine)	–	–
Configura azioni personalizzate	Attuali	Attuali	Attuali
Configura le regole di automazione	Qualsiasi	–	–
Configura approfondimenti personalizzati	Attuali	Attuali	Attuali

Azioni consentite se si esegue l'integrazione con Organizations e si utilizza la configurazione locale

Gli account amministratore e membro possono accedere alle azioni CSPM di Security Hub come segue se si effettua l'integrazione con Organizations e si utilizza la configurazione locale.

Azione	Account amministratore delegato Security Hub CSPM	Account membro
Creare e gestire le politiche di configurazione CSPM di Security Hub	–	–
Visualizza gli account dell'organizzazione	Qualsiasi	–

Azione	Account amministratore delegato Security Hub CSPM	Account membro
Account socio dissociato	Qualsiasi	–
Eliminare l'account del membro	–	–
Disattiva Security Hub CSPM	–	Corrente (se l'account non è associato all'amministratore delegato)
Visualizza i risultati e la cronologia delle scoperte	Qualsiasi	Attuali
Aggiorna i risultati	Qualsiasi	Attuali
Visualizza i risultati delle analisi	Qualsiasi	Attuali
Visualizza i dettagli del controllo	Qualsiasi	Attuali
Attiva o disattiva i risultati del controllo consolidato	Qualsiasi	–
Abilita e disabilita gli standard	Attuali	Attuali
Abilita automaticamente Security Hub, CSPM e gli standard predefiniti nei nuovi account dell'organizzazione	Per account correnti e nuovi account aziendali	–
Abilita e disabilita i controlli	Attuali	Attuali
Abilita e disabilita le integrazioni	Attuali	Attuali
Configura l'aggregazione tra regioni	Qualsiasi	–

Azione	Account amministratore delegato Security Hub CSPM	Account membro
Configura azioni personalizzate	Attuali	Attuali
Configura le regole di automazione	Qualsiasi	–
Configura approfondimenti personalizzati	Attuali	Attuali

Azioni consentite per gli account basati su invito

Gli account amministratore e membro possono accedere alle azioni CSPM di Security Hub come segue se si utilizza il metodo basato su invito per gestire manualmente gli account anziché integrarli con. AWS Organizations

Azione	Account amministratore CSPM di Security Hub	Account membro
Creare e gestire le politiche di configurazione CSPM di Security Hub	–	–
Visualizza gli account dell'organizzazione	Qualsiasi	–
Account socio dissociato	Qualsiasi	Attuali
Eliminare l'account del membro	Qualsiasi	–
Disattiva Security Hub CSPM	Attuale (se non ci sono account membri abilitati)	Corrente (se l'account è dissociato dall'account amministratore)

Azione	Account amministratore CSPM di Security Hub	Account membro
Visualizza i risultati e la cronologia delle scoperte	Qualsiasi	Attuali
Aggiorna i risultati	Qualsiasi	Attuali
Visualizza i risultati delle analisi	Qualsiasi	Attuali
Visualizza i dettagli del controllo	Qualsiasi	Attuali
Attiva o disattiva i risultati del controllo consolidato	Qualsiasi	–
Abilita e disabilita gli standard	Attuali	Attuali
Abilita automaticamente Security Hub, CSPM e gli standard predefiniti nei nuovi account dell'organizzazione	–	–
Abilita e disabilita i controlli	Attuali	Attuali
Abilita e disabilita le integrazioni	Attuali	Attuali
Configura l'aggregazione tra regioni	Qualsiasi	–
Configura azioni personalizzate	Attuali	Attuali
Configura le regole di automazione	Qualsiasi	–
Configura approfondimenti personalizzati	Attuali	Attuali

Effetto delle azioni dell'account sui dati CSPM di Security Hub

Queste azioni dell'account hanno i seguenti effetti sui dati CSPM AWS di Security Hub.

Security Hub CSPM disabilitato

Se si utilizza la configurazione centrale, l'amministratore delegato (DA) può creare politiche di configurazione CSPM di Security Hub che disabilitano AWS Security Hub CSPM in account e unità organizzative (OU) specifici. In questo caso, Security Hub CSPM è disabilitato negli account e nelle unità organizzative specificati nella regione di residenza e in tutte le regioni collegate. Se non utilizzi la configurazione centrale, devi disabilitare Security Hub CSPM separatamente in ogni account e regione in cui l'hai abilitato. Non è possibile utilizzare la configurazione centrale se Security Hub CSPM è disabilitato nell'account DA.

Nessun risultato viene generato o aggiornato per l'account amministratore se Security Hub CSPM è disabilitato nell'account amministratore. I risultati archiviati esistenti vengono eliminati dopo 30 giorni. I risultati attivi esistenti vengono eliminati dopo 90 giorni.

Le integrazioni con altri Servizi AWS vengono rimosse.

Gli standard e i controlli di sicurezza abilitati sono disabilitati.

Altri dati e impostazioni CSPM di Security Hub, tra cui azioni personalizzate, approfondimenti e abbonamenti a prodotti di terze parti, vengono conservati per 90 giorni.

Account membro dissociato dall'account amministratore

Quando un account membro viene dissociato dall'account amministratore, l'account amministratore perde l'autorizzazione a visualizzare i risultati nell'account membro. Tuttavia, Security Hub CSPM è ancora abilitato in entrambi gli account.

Se si utilizza la configurazione centrale, il DA non può configurare Security Hub CSPM per un account membro dissociato dall'account DA.

Le impostazioni o le integrazioni personalizzate definite per l'account amministratore non vengono applicate ai risultati dell'account precedente. Ad esempio, dopo la dissociazione degli account, potresti avere un'azione personalizzata nell'account amministratore utilizzato come modello di evento in una EventBridge regola Amazon. Tuttavia, questa azione personalizzata non può essere utilizzata nell'account del membro.

Nell'elenco Account per l'account amministratore CSPM di Security Hub, un account rimosso ha lo stato Disassociato.

L'account membro viene rimosso da un'organizzazione

Quando un account membro viene rimosso da un'organizzazione, l'account amministratore CSPM di Security Hub perde l'autorizzazione a visualizzare i risultati nell'account membro. Tuttavia, Security Hub CSPM è ancora abilitato in entrambi gli account con le stesse impostazioni che avevano prima della rimozione.

Se utilizzi la configurazione centrale, non puoi configurare Security Hub CSPM per un account membro dopo che è stato rimosso dall'organizzazione a cui appartiene l'amministratore delegato. Tuttavia, l'account mantiene le impostazioni che aveva prima della rimozione, a meno che non vengano modificate manualmente.

Nell'elenco Account per l'account amministratore CSPM di Security Hub, un account rimosso ha lo stato Eliminato.

L'account è sospeso

Quando un account Account AWS viene sospeso, l'account perde l'autorizzazione a visualizzare i risultati in Security Hub CSPM. Nessun risultato viene generato o aggiornato per quell'account. L'account amministratore di un account sospeso può visualizzare i risultati esistenti relativi all'account.

Per un account dell'organizzazione, lo stato dell'account membro può anche cambiare in Account sospeso. Ciò accade se l'account viene sospeso nello stesso momento in cui l'account amministratore tenta di abilitarlo. L'account amministratore di un account sospeso non può visualizzare i risultati relativi a quell'account. Altrimenti, lo stato di sospensione non influisce sullo stato dell'account membro.

Se si utilizza la configurazione centrale, l'associazione delle politiche fallisce se l'amministratore delegato tenta di associare una politica di configurazione a un account sospeso.

Dopo 90 giorni, l'account viene chiuso o riattivato. Quando l'account viene riattivato, le autorizzazioni CSPM del Security Hub vengono ripristinate. Se lo stato dell'account membro è Account sospeso, l'account amministratore deve abilitare l'account manualmente.

L'account è chiuso

Quando un Account AWS è chiuso, Security Hub CSPM risponde alla chiusura come segue.

Se l'account è un account amministratore CSPM di Security Hub, viene rimosso come account amministratore e tutti gli account dei membri vengono rimossi. Se l'account è un account membro, viene dissociato e rimosso come membro dall'account amministratore CSPM di Security Hub.

Security Hub CSPM conserva i risultati archiviati esistenti nell'account per 30 giorni. Per un risultato di controllo, il calcolo di 30 giorni si basa sul valore del `UpdatedAt` campo del risultato. Per un altro tipo di risultato, il calcolo si basa sul valore del `ProcessedAt` campo `UpdatedAt` o del risultato, a seconda di quale data sia più recente. Al termine di questo periodo di 30 giorni, Security Hub CSPM elimina definitivamente i risultati dall'account.

Security Hub CSPM conserva i risultati attivi esistenti nell'account per 90 giorni. Per un risultato di controllo, il calcolo di 90 giorni si basa sul valore del `UpdatedAt` campo del risultato. Per un altro tipo di risultato, il calcolo si basa sul valore del `ProcessedAt` campo `UpdatedAt` o del risultato, a seconda di quale data sia più recente. Al termine di questo periodo di 90 giorni, Security Hub CSPM elimina definitivamente i risultati dall'account.

Per conservare a lungo termine i risultati esistenti, puoi esportare i risultati in un bucket S3. Puoi farlo utilizzando un'azione personalizzata con una EventBridge regola Amazon. Per ulteriori informazioni, consulta Utilizzo EventBridge per la risposta e la correzione automatiche.

> **Important**
>
> Per i clienti registratiAWS GovCloud (US) Regions, esegui il backup e quindi elimina i dati della polizza e altre risorse dell'account prima di chiudere l'account. Non avrai accesso alle risorse e ai dati dopo la chiusura dell'account.

Per ulteriori informazioni, consulta Close an Account AWS nella Guida Gestione dell'account AWS di riferimento.

Comprendere l'aggregazione interregionale in Security Hub CSPM

> **Note**
>
> La regione di aggregazione è ora denominata regione principale. Alcune operazioni dell'API CSPM di Security Hub utilizzano ancora la regione di aggregazione con termini precedenti.

Utilizzando l'aggregazione interregionale in AWS Security Hub CSPM, puoi aggregare i risultati, trovare aggiornamenti, approfondimenti, controllare gli stati di conformità e i punteggi di sicurezza da più Regioni AWS aree geografiche a un'unica area geografica. È quindi possibile gestire tutti questi dati dalla regione di origine.

Supponiamo di impostare Stati Uniti orientali (Virginia settentrionale) come regione di origine e Stati Uniti occidentali (Oregon) e Stati Uniti occidentali (California settentrionale) come regioni collegate. Quando si visualizza la pagina Risultati negli Stati Uniti orientali (Virginia settentrionale), vengono visualizzati i risultati di tutte e tre le regioni. Gli aggiornamenti a tali risultati si riflettono anche in tutte e tre le regioni.

> **Note**
>
> InAWS GovCloud (US), l'aggregazione tra regioni è supportata solo per i risultati, gli aggiornamenti delle ricerche e gli approfondimenti in tutte le aree. AWS GovCloud (US) In particolare, puoi aggregare i risultati, trovare aggiornamenti e approfondimenti solo tra AWS GovCloud (US-East) e AWS GovCloud (). US-West Nelle regioni della Cina, l'aggregazione interregionale è supportata solo per i risultati, gli aggiornamenti delle ricerche e gli approfondimenti nelle regioni della Cina. In particolare, puoi solo aggregare risultati, trovare aggiornamenti e approfondimenti tra Cina (Pechino) e Cina (Ningxia).

Se un controllo è abilitato in una regione collegata ma disattivato nella regione di origine, è possibile visualizzare lo stato di conformità del controllo dalla regione di origine, ma non è possibile abilitare o disabilitare tale controllo dalla regione di origine. L'eccezione è se si utilizza la configurazione centrale. Se si utilizza la configurazione centrale, l'amministratore delegato di Security Hub CSPM può configurare i controlli nella regione di origine e nelle regioni collegate dalla regione di origine.

Se hai impostato una regione d'origine, i punteggi di sicurezza tengono conto degli stati di controllo in generale Regioni collegate. Per visualizzare i punteggi di sicurezza e gli stati di conformità tra le regioni, aggiungi le seguenti autorizzazioni al tuo ruolo IAM che utilizza Security Hub CSPM:

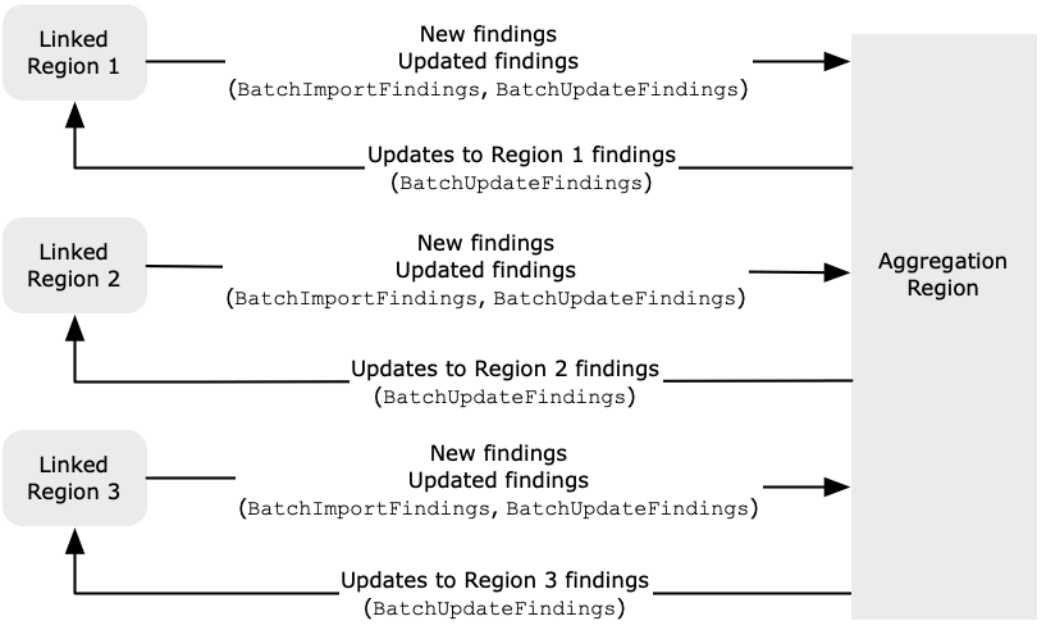
- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

Tipi di dati aggregati

Quando l'aggregazione tra regioni è abilitata con una o più regioni collegate, Security Hub CSPM replica i seguenti dati dalle regioni collegate alla regione principale. Ciò si verifica in tutti gli account in cui è abilitata l'aggregazione tra regioni.

- Esiti
- Approfondimenti
- Controlla gli stati di conformità
- Punteggi di sicurezza

Oltre ai nuovi dati nell'elenco precedente, Security Hub CSPM replica anche gli aggiornamenti di questi dati tra le regioni collegate e la regione principale. Gli aggiornamenti che si verificano in una regione collegata vengono replicati nella regione di origine. Gli aggiornamenti che si verificano nella regione di origine vengono replicati nella regione collegata. Se sono presenti aggiornamenti in conflitto nella regione di origine e nella regione collegata, viene utilizzato l'aggiornamento più recente.



Cross-Region l'aggregazione non aumenta il costo del Security Hub CSPM. Non ti viene addebitato alcun costo quando Security Hub CSPM replica nuovi dati o aggiornamenti.

Nella regione di origine, la pagina di riepilogo fornisce una visualizzazione dei risultati attivi nelle regioni collegate. Per informazioni, vedere Visualizzazione di un riepilogo interregionale dei risultati

per gravità. In altri pannelli della pagina di riepilogo che analizzano i risultati vengono visualizzate anche informazioni provenienti da tutte le regioni collegate.

I punteggi di sicurezza nella regione d'origine vengono calcolati confrontando il numero di controlli approvati con il numero di controlli abilitati in tutte le aree collegate. Inoltre, se un controllo è abilitato in almeno una regione collegata, è visibile nelle pagine dei dettagli degli standard di sicurezza della regione d'origine. Lo stato di conformità dei controlli nelle pagine dei dettagli degli standard riflette i risultati delle regioni collegate. Se un controllo di sicurezza associato a un controllo ha esito negativo in una o più aree collegate, lo stato di conformità di tale controllo viene visualizzato come Non riuscito nelle pagine dei dettagli degli standard della regione di origine. Il numero di controlli di sicurezza include i risultati di tutte le regioni collegate.

Security Hub CSPM aggrega solo i dati delle regioni in cui un account ha il Security Hub CSPM abilitato. Security Hub CSPM non è abilitato automaticamente per un account in base alla configurazione di aggregazione tra regioni.

È possibile abilitare l'aggregazione tra regioni senza selezionare alcuna regione collegata. In questo caso, non si verifica alcuna replica dei dati.

Aggregazione per gli account degli amministratori e dei membri

Gli account autonomi, gli account membro e gli account amministratore possono configurare l'aggregazione tra regioni. Se configurata da un amministratore, la presenza dell'account amministratore è essenziale affinché l'aggregazione tra regioni funzioni negli account amministrati. Se l'account amministratore viene rimosso o dissociato da un account membro, l'aggregazione tra aree geografiche per l'account membro si interrompe. Ciò è vero anche se l'aggregazione tra aree geografiche era abilitata per l'account prima dell'inizio della relazione amministratore-membro.

Quando un account amministratore abilita l'aggregazione tra regioni, Security Hub CSPM replica i dati generati dall'account amministratore in tutte le regioni collegate alla regione di origine. Inoltre, Security Hub CSPM identifica gli account membro associati a quell'amministratore e ogni account membro eredita le impostazioni di aggregazione interregionale dell'amministratore. Security Hub CSPM replica i dati generati da un account membro in tutte le regioni collegate alla regione di origine.

L'amministratore può accedere e gestire i risultati di sicurezza di tutti gli account dei membri all'interno delle regioni amministrate. Tuttavia, in qualità di amministratore CSPM di Security Hub, devi accedere alla regione di origine per visualizzare i dati aggregati di tutti gli account membri e le regioni collegate.

In qualità di account membro del Security Hub CSPM, devi accedere alla regione d'origine per visualizzare i dati aggregati del tuo account da tutte le regioni collegate. Gli account dei membri non dispongono delle autorizzazioni per visualizzare i dati degli altri account membri.

Un account amministratore può invitare manualmente gli account dei membri o fungere da amministratore delegato di un'organizzazione integrata con. AWS Organizations Per un account membro invitato manualmente, l'amministratore deve invitare l'account dalla regione di origine e da tutte le regioni collegate affinché l'aggregazione tra regioni funzioni. Inoltre, l'account membro deve avere il Security Hub CSPM abilitato nella regione di origine e in tutte le regioni collegate per consentire all'amministratore di visualizzare i risultati dell'account membro. Se non utilizzi la regione d'origine per altri scopi, puoi disabilitare gli standard e le integrazioni CSPM di Security Hub in quella regione per evitare addebiti.

Se prevedi di utilizzare l'aggregazione tra regioni e disponi di più account amministratore, ti consigliamo di seguire queste best practice:

- Ogni account amministratore ha account membri diversi.
- Ogni account amministratore ha gli stessi account membro in tutte le regioni.
- Ogni account amministratore utilizza una regione di residenza diversa.

> **Note**
>
> Per capire in che modo l'aggregazione tra regioni influisce sulla configurazione centrale, consulta. Impatto della configurazione centrale sull'aggregazione tra regioni

Impatto della configurazione centrale sull'aggregazione tra regioni

La configurazione centrale è una funzionalità opzionale di AWS Security Hub CSPM che puoi utilizzare se esegui l'integrazione con. AWS Organizations Se si utilizza la configurazione centrale, l'account amministratore delegato può configurare il servizio CSPM, gli standard e i controlli di Security Hub per gli account e le unità organizzative (OU) dell'organizzazione. Per configurare account e unità organizzative, l'amministratore delegato crea politiche di configurazione CSPM di Security Hub. Le policy di configurazione possono essere utilizzate per definire se Security Hub CSPM è abilitato o disabilitato e quali standard e controlli sono abilitati. L'amministratore delegato associa le politiche di configurazione a account specifici, unità organizzative o alla radice (l'intera organizzazione).

L'amministratore delegato può creare e gestire le politiche di configurazione per l'organizzazione solo dalla regione di origine. Inoltre, le politiche di configurazione hanno effetto nella regione di origine e in tutte le regioni collegate. Non è possibile creare una politica di configurazione che si applichi solo in alcune regioni collegate e non in altre. Per informazioni sull'aggregazione tra regioni, vedi Cross-Region aggregazione.

Per utilizzare la configurazione centralizzata, è necessario designare una regione di residenza. Facoltativamente, puoi scegliere una o più regioni come regioni collegate. Puoi anche scegliere di designare una regione d'origine senza alcuna regione collegata.

La modifica delle impostazioni di aggregazione tra regioni può influire sulle politiche di configurazione. Quando aggiungi una regione collegata, le tue politiche di configurazione hanno effetto in quella regione. Se la Regione è una regione opzionale, deve essere abilitata affinché le politiche di configurazione abbiano effetto in quella regione. Al contrario, quando rimuovi una regione collegata, le politiche di configurazione non hanno più effetto in quella regione. In quella regione, gli account mantengono le impostazioni che avevano quando la regione collegata è stata rimossa. È possibile modificare tali impostazioni, ma è necessario farlo separatamente in ogni account e regione.

Se si rimuove o si modifica la regione di origine, i criteri di configurazione e le associazioni di criteri vengono eliminati. Non è più possibile utilizzare la configurazione centrale o creare politiche di configurazione in nessuna regione. Gli account mantengono le impostazioni che avevano prima che la regione di origine venisse modificata o rimossa. È possibile modificare tali impostazioni in qualsiasi momento, ma poiché non si utilizza più la configurazione centrale, le impostazioni devono essere modificate separatamente in ogni account e regione. È possibile utilizzare la configurazione centrale e creare nuovamente politiche di configurazione se si designa una nuova regione di residenza.

Per ulteriori informazioni sulla configurazione centrale, vedereComprendere la configurazione centrale in Security Hub CSPM.

Abilitazione dell'aggregazione tra regioni

> **Note**
>
> La regione di aggregazione è ora denominata regione di origine. Alcune operazioni dell'API CSPM di Security Hub utilizzano ancora la regione di aggregazione con termini precedenti.

È necessario abilitare l'aggregazione tra le regioni dalla regione Regione AWS che si desidera designare come area di origine.

Per abilitare l'aggregazione tra regioni, si crea una risorsa CSPM Security Hub denominata aggregatore di ricerca. La risorsa Finding Aggregator specifica la tua regione di origine e le regioni collegate (se presenti).

Non puoi utilizzare una Regione AWS regione disabilitata per impostazione predefinita come regione d'origine. Per un elenco delle regioni disabilitate per impostazione predefinita, vedi Abilitazione di una regione in Riferimenti generali di AWS.

Quando abiliti l'aggregazione tra regioni, scegli di specificare una o più regioni collegate, se lo desideri. Puoi anche scegliere se collegare automaticamente le nuove regioni quando Security Hub CSPM inizia a supportarle e le hai accettate.

Security Hub CSPM console

Per abilitare l'aggregazione tra regioni

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Utilizzando il Regione AWS selettore, accedi alla regione che desideri utilizzare come regione di aggregazione.
3. Nel menu di navigazione CSPM di Security Hub, scegli Impostazioni e poi Regioni.
4. Per Finding aggregation, scegli Configura aggregazione di risultati.

   Per impostazione predefinita, la regione principale è impostata su Nessuna regione di aggregazione.
5. In Regione di aggregazione, seleziona l'opzione per designare la regione corrente come regione di origine.
6. Facoltativamente, per le regioni collegate, seleziona le regioni da cui aggregare i dati.
7. Per aggregare automaticamente i dati provenienti da nuove regioni nella partizione supportate da Security Hub CSPM e per attivarle, seleziona Collega regioni future.
8. Scegli Save (Salva).

Security Hub CSPM API

Dalla regione che desideri utilizzare come regione principale, utilizza il `CreateFindingAggregator`funzionamento dell'API CSPM Security Hub. Se utilizzi ilAWS CLI, esegui il comando create-finding-aggregator.

Per `RegionLinkingMode`, scegliere una delle seguenti opzioni:

- `ALL_REGIONS`— Security Hub CSPM aggrega i dati di tutte le regioni. Security Hub CSPM aggrega anche i dati provenienti da nuove regioni man mano che sono supportate e l'utente le accetta.
- `ALL_REGIONS_EXCEPT_SPECIFIED`— Security Hub CSPM aggrega i dati di tutte le regioni ad eccezione delle regioni che si desidera escludere. Security Hub CSPM aggrega anche i dati provenienti da nuove regioni man mano che sono supportate e l'utente le accetta. Utilizzare `Regions` per fornire l'elenco delle regioni da escludere dall'aggregazione.
- `SPECIFIED_REGIONS`— Security Hub CSPM aggrega i dati da un elenco selezionato di regioni. Security Hub CSPM non aggrega automaticamente i dati provenienti da nuove regioni. `Regions`Da utilizzare per fornire l'elenco delle regioni da cui eseguire l'aggregazione.
- `NO_REGIONS`— Security Hub CSPM non aggrega i dati perché non selezioni alcuna regione collegata.

L'esempio seguente configura l'aggregazione tra regioni. La regione di origine è Stati Uniti orientali (Virginia settentrionale). Le regioni collegate sono Stati Uniti occidentali (California settentrionale) e Stati Uniti occidentali (Oregon). Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub create-finding-aggregator --region us-east-1 --region-linking-
mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Revisione delle impostazioni di aggregazione tra regioni

> **Note**
>
> La regione di aggregazione è ora denominata regione di origine. Alcune operazioni dell'API CSPM di Security Hub utilizzano ancora la regione di aggregazione con termini precedenti.

È possibile visualizzare l'attuale configurazione di aggregazione interregionale in AWS Security Hub CSPM da qualsiasi. Regione AWS La configurazione include la regione principale, le regioni collegate (se presenti) e se collegare automaticamente le nuove regioni poiché Security Hub CSPM le supporta.

Gli account membro possono visualizzare le impostazioni di aggregazione tra le regioni configurate dall'account amministratore.

Scegli il tuo metodo preferito e segui i passaggi per visualizzare le impostazioni correnti di aggregazione tra le regioni.

Security Hub CSPM console

Per visualizzare le impostazioni di aggregazione tra regioni (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Impostazioni, quindi la scheda Regioni.

Se l'aggregazione tra regioni non è abilitata, nella scheda Regioni viene visualizzata l'opzione per abilitare l'aggregazione tra regioni. Solo gli account amministratore e gli account autonomi possono abilitare l'aggregazione tra regioni.

Se l'aggregazione tra regioni è abilitata, la scheda Regioni visualizza le seguenti informazioni:

- La regione di origine
- Se aggregare automaticamente risultati, approfondimenti, stati di controllo e punteggi di sicurezza provenienti da nuove regioni supportate da Security Hub CSPM e per le quali hai scelto di aderire
- L'elenco delle regioni collegate (se selezionate)

Security Hub CSPM API

Per esaminare le impostazioni di aggregazione tra regioni (API CSPM Security Hub)

Utilizza il `GetFindingAggregator`funzionamento dell'API CSPM Security Hub. Se utilizzi ilAWS CLI, esegui il comando get-finding-aggregator.

Quando effettui la richiesta, fornisci l'ARN dell'aggregatore di ricerca. Per ottenere l'ARN dell'aggregatore di ricerca, utilizzare l'operazione o `ListFindingAggregators`il comando list-finding-aggregators.

L'esempio seguente mostra le impostazioni di aggregazione tra regioni per l'ARN dell'aggregatore di ricerca specificato. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di riga rovesciata (\) per migliorare la leggibilità

```
$aws securityhub get-finding-aggregator --finding-aggregator-
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-
e89b-12d3-a456-426652340000
```

Aggiornamento delle impostazioni di aggregazione tra regioni

> **Note**
>
> La regione di aggregazione è ora denominata regione di origine. Alcune operazioni dell'API CSPM di Security Hub utilizzano ancora la regione di aggregazione con termini precedenti.

Puoi aggiornare le impostazioni correnti di aggregazione interregionale in AWS Security Hub CSPM modificando le Regioni collegate o la regione principale corrente. È inoltre possibile modificare se aggregare automaticamente i dati da quelli nuovi in Regioni AWS cui è supportato Security Hub CSPM.

Le modifiche all'aggregazione tra aree geografiche non vengono implementate per una regione opt-in finché non abiliti la regione nella tua. Account AWS Le regioni AWS introdotte a partire dal 20 marzo 2019 o in data successiva sono regioni opzionali.

Quando interrompi l'aggregazione dei dati da una regione collegata, AWS Security Hub CSPM non rimuove alcun dato aggregato esistente da quella regione accessibile nella regione di origine.

Non è possibile utilizzare le procedure di aggiornamento in questa sezione per modificare la regione di origine. Per cambiare la regione d'origine, devi fare quanto segue:

1. Interrompi l'aggregazione tra regioni. Per istruzioni, consulta the section called “Interruzione dell'aggregazione”.
2. Passa alla regione che desideri utilizzare come nuova regione di origine.
3. Abilita l'aggregazione tra regioni. Per istruzioni, consulta the section called “Abilitare l'aggregazione”.

È necessario aggiornare la configurazione di aggregazione tra aree geografiche dalla regione principale corrente.

Security Hub CSPM console

Per modificare le regioni collegate

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi alla regione di aggregazione corrente.
2. Nel menu di navigazione CSPM di Security Hub, scegli Impostazioni, quindi scegli Regioni.
3. Per Trovare l'aggregazione, scegli Modifica.
4. Per le regioni collegate, aggiorna le aree collegate selezionate.
5. Se necessario, cambia se è selezionata l'opzione Collega regioni future. Questa impostazione determina se Security Hub CSPM collega automaticamente le nuove regioni man mano che ne aggiunge il supporto e l'utente le accetta.
6. Scegli Save (Salva).

Security Hub CSPM API

Usa l'operazione. `UpdateFindingAggregator` Se si utilizza ilAWS CLI, eseguire il comando update-finding-aggregator. Per identificare l'aggregatore di risultati, è necessario fornire l'ARN dell'aggregatore di risultati. Per ottenere l'ARN dell'aggregatore di ricerca, utilizzare l'operazione o `ListFindingAggregators`il comando list-finding-aggregators..

Se la modalità di collegamento è o, è possibile modificare l'elenco delle `ALL_REGIONS_EXCEPT_SPECIFIED` regioni `SPECIFIED_REGIONS` escluse o incluse. Se desideri modificare la modalità di collegamento delle regioni in`NO_REGIONS`, non dovresti fornire un elenco di regioni.

Quando modifichi l'elenco delle regioni escluse o incluse, devi fornire l'elenco completo con gli aggiornamenti. Ad esempio, supponiamo che attualmente tu voglia aggregare i risultati degli Stati Uniti orientali (Ohio) e di voler aggregare anche i risultati degli Stati Uniti occidentali (Oregon). È necessario fornire un `Regions` elenco che contenga sia Stati Uniti orientali (Ohio) che Stati Uniti occidentali (Oregon).

L'esempio seguente aggiorna l'aggregazione tra regioni alle regioni selezionate. Il comando viene eseguito dalla regione di origine corrente, che è Stati Uniti orientali (Virginia settentrionale). Le regioni collegate sono Stati Uniti occidentali (California settentrionale) e Stati Uniti occidentali (Oregon). Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
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
```

Interruzione dell'aggregazione tra regioni

> **Note**
>
> La regione di aggregazione è ora denominata regione di origine. Alcune operazioni dell'API CSPM di Security Hub utilizzano ancora la regione di aggregazione con termini precedenti.

Se non desideri che AWS Security Hub CSPM aggreghi i dati, puoi eliminare il tuo aggregatore di risultati. In alternativa, puoi mantenere l'aggregatore di risultati ma non collegarne nessuno Regioni AWS alla regione di origine aggiornando l'aggregatore esistente alla modalità di collegamento. `NO_REGIONS`

Per cambiare la tua regione di residenza, devi eliminare l'attuale aggregatore di risultati e crearne uno nuovo.

Quando elimini il tuo aggregatore di risultati, Security Hub CSPM interrompe l'aggregazione dei dati. Non rimuove alcun dato aggregato esistente dalla regione di origine.

Eliminazione dell'aggregatore di ricerca (console)

Puoi eliminare l'aggregatore di risultati solo dalla regione di residenza corrente.

Nelle regioni diverse dalla regione di origine, il pannello di aggregazione Finding sulla console CSPM di Security Hub visualizza un messaggio che indica che è necessario modificare la configurazione nella regione di origine. Scegli questo messaggio per visualizzare un collegamento per passare alla regione d'origine.

Security Hub CSPM console

Per interrompere l'aggregazione tra regioni (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Assicurati di aver effettuato l'accesso alla tua regione di residenza attuale.
3. Nel menu di navigazione CSPM di Security Hub, scegli Impostazioni, quindi scegli Regioni.
4. In Ricerca di aggregazione, scegli Modifica.
5. In Regione di aggregazione, scegli Nessuna regione di aggregazione.
6. Scegli Save (Salva).
7. Nella finestra di dialogo di conferma, nel campo di conferma, digita. **`Confirm`**
8. Scegli Conferma.

Security Hub CSPM API

Utilizza il `DeleteFindingAggregator`funzionamento dell'API CSPM Security Hub. Se stai usandoAWS CLI, esegui il comando. `delete-finding-aggregator`

Per identificare l'aggregatore di risultati da eliminare, fornisci l'ARN dell'aggregatore di risultati. Per ottenere l'ARN dell'aggregatore di ricerca, utilizzare l'operazione o `ListFindingAggregators`il comando `list-finding-aggregators`.

L'esempio seguente elimina l'aggregatore di ricerca. Il comando viene eseguito dalla regione di origine corrente, ovvero Stati Uniti orientali (Virginia settentrionale). Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --region us-east-1
```

Comprensione degli standard di sicurezza in Security Hub CSPM

In AWS Security Hub CSPM, uno standard di sicurezza è un insieme di requisiti basati su quadri normativi, best practice del settore o politiche aziendali. Per i dettagli sugli standard attualmente

supportati da Security Hub CSPM, inclusi i controlli di sicurezza che si applicano a ciascuno di essi, vedere il. Riferimento agli standard per Security Hub CSPM

Quando abiliti uno standard, Security Hub CSPM abilita automaticamente tutti i controlli che si applicano allo standard. Security Hub CSPM esegue quindi controlli di sicurezza sui controlli, che generano i risultati CSPM di Security Hub. È possibile disabilitare e riattivare successivamente i singoli controlli, se necessario. È inoltre possibile disabilitare completamente uno standard. Se disabiliti uno standard, Security Hub CSPM interrompe l'esecuzione dei controlli di sicurezza sui controlli che si applicano allo standard. I risultati non vengono più generati per i controlli.

Oltre ai risultati, Security Hub CSPM genera un punteggio di sicurezza per ogni standard abilitato. Il punteggio si basa sullo stato dei controlli che si applicano allo standard. Se imposti una regione di aggregazione, il punteggio di sicurezza per uno standard riflette lo stato dei controlli in tutte le regioni collegate. Se sei l'amministratore CSPM di Security Hub per un'organizzazione, il punteggio riflette lo stato dei controlli per tutti gli account dell'organizzazione. Per ulteriori informazioni, consulta Calcolo dei punteggi di sicurezza.

Per rivedere e gestire gli standard, puoi utilizzare la console CSPM di Security Hub o l'API CSPM di Security Hub. Sulla console, la pagina degli standard di sicurezza mostra tutti gli standard di sicurezza attualmente supportati da Security Hub CSPM. Ciò include una descrizione di ogni standard e lo stato attuale dello standard. Se abiliti uno standard, puoi utilizzare questa pagina anche per accedere a dettagli aggiuntivi sullo standard. Ad esempio, puoi rivedere:

- Il punteggio di sicurezza attuale dello standard.
- Statistiche aggregate per i controlli che si applicano allo standard.
- Un elenco di controlli che si applicano allo standard e che sono attualmente abilitati, incluso lo stato di conformità di ciascuno di essi.
- Un elenco di controlli che si applicano allo standard ma che sono attualmente disabilitati.

Per un'analisi più approfondita, puoi filtrare e ordinare i dati e approfondire i dettagli dei singoli controlli che si applicano allo standard.

È possibile abilitare gli standard singolarmente per un singolo account e Regione AWS. Tuttavia, per risparmiare tempo e ridurre le variazioni di configurazione in ambienti con più account e più regioni, consigliamo di utilizzare la configurazione centrale per abilitare e gestire gli standard. Con la configurazione centralizzata, l'amministratore delegato di Security Hub CSPM può creare politiche che specificano come configurare uno standard su più account e regioni.

Argomenti

- Riferimento agli standard per Security Hub CSPM
- Abilitazione di uno standard di sicurezza
- Revisione dei dettagli di uno standard di sicurezza
- Disattivazione degli standard di sicurezza abilitati automaticamente
- Disabilitazione di uno standard di sicurezza

Riferimento agli standard per Security Hub CSPM

In AWS Security Hub CSPM, uno standard di sicurezza è un insieme di requisiti basati su quadri normativi, best practice del settore o politiche aziendali. Security Hub CSPM associa questi requisiti ai controlli ed esegue controlli di sicurezza sui controlli per valutare se i requisiti di uno standard sono soddisfatti. Ogni standard include più controlli.

Security Hub CSPM attualmente supporta i seguenti standard:

- AWS Best practice di sicurezza di base: sviluppato da AWS professionisti del settore, questo standard è una raccolta di best practice di sicurezza per le organizzazioni, indipendentemente dal settore o dalle dimensioni. Fornisce una serie di controlli che rilevano quando le tue Account AWS risorse si discostano dalle migliori pratiche di sicurezza. Fornisce inoltre indicazioni prescrittive su come migliorare e mantenere il livello di sicurezza.
- Best practice per la sicurezza dell'IA: sviluppato da esperti AWS di sicurezza, questo standard fornisce una serie curata di controlli che rilevano quando le risorse di intelligenza artificiale distribuite non sono in linea con le migliori pratiche di sicurezza. Ti aiuta a identificare le aree in cui i carichi di lavoro AI si discostano dalle configurazioni di sicurezza consigliate, coprendo domini come l'isolamento della rete, la crittografia, il posizionamento dei VPC e l'utilizzo delle chiavi. AWS KMS
- AWS Etichettatura delle risorse: sviluppato da Security Hub CSPM, questo standard può aiutarti a determinare se AWS le tue risorse dispongono di tag. Un tag è una coppia chiave-valore che funge da metadati per una risorsa. AWS I tag possono aiutarti a identificare, classificare, gestire e cercare risorse. AWS Ad esempio, puoi utilizzare i tag per classificare le risorse in base allo scopo, al proprietario o all'ambiente.
- CIS AWS Foundations Benchmark — Sviluppato dal Center for Internet Security (CIS), questo standard fornisce linee guida di configurazione sicure per. AWS Specifica una serie di linee guida e best practice per la configurazione della sicurezza per un sottoinsieme di risorse, con particolare

attenzione alle impostazioni di base, verificabili Servizi AWS e indipendenti dall'architettura. Le linee guida includono procedure di implementazione e valutazione chiare e dettagliate.

- NIST SP 800-53 Revisione 5 — Questo standard è in linea con i requisiti del National Institute of Standards and Technology (NIST) per proteggere la riservatezza, l'integrità e la disponibilità dei sistemi di informazione e delle risorse critiche. Il quadro associato si applica generalmente alle agenzie federali o alle U.S organizzazioni che collaborano con agenzie federali o sistemi di informazione U.S. Tuttavia, le organizzazioni private possono utilizzare i requisiti anche come quadro guida.
- NIST SP 800-171 Revisione 2 — Questo standard è in linea con le raccomandazioni e i requisiti di sicurezza del NIST per proteggere la riservatezza delle informazioni controllate non classificate (CUI) in sistemi e organizzazioni che non fanno parte del governo federale. U.S Le CUI sono informazioni che non soddisfano i criteri di classificazione governativi, ma sono considerate sensibili e sono create o possedute dal governo federale o da altre entità per conto del governo federale U.S. U.S
- PCI DSS: questo standard si allinea al framework di conformità PCI DSS (Payment Card Industry Data Security Standard) definito dal PCI Security Standards Council (SSC). Il framework fornisce una serie di regole e linee guida per la gestione sicura dei dati delle carte di credito e di debito. Il framework si applica generalmente alle organizzazioni che archiviano, elaborano o trasmettono i dati dei titolari di carte.
- CRI Profile v2.2 — Questo standard è in linea con il CRI Profile, un framework di conformità sviluppato dal Cyber Risk Institute (CRI). Il framework armonizza la sicurezza informatica e le aspettative normative che si applicano al settore dei servizi finanziari in una serie di requisiti comuni. Il quadro si applica generalmente agli istituti finanziari e alle organizzazioni che li servono.
- Service-managed standard, AWS Control Tower — Questo standard consente di configurare i controlli di rilevamento forniti da Security Hub CSPM. AWS Control Tower AWS Control Tower offre un modo semplice per configurare e gestire un ambiente AWS multi-account, seguendo le migliori pratiche prescrittive.

Gli standard e i controlli CSPM di Security Hub non garantiscono la conformità a nessun quadro normativo o controllo. Al contrario, forniscono un modo per valutare e monitorare lo stato delle vostre risorse. Account AWS Ti consigliamo di abilitare ogni standard pertinente alle tue esigenze aziendali, al tuo settore o al tuo caso d'uso.

I singoli controlli possono essere applicati a più di uno standard. Se abiliti più standard, ti consigliamo di abilitare anche i risultati di controllo consolidati. In tal caso, Security Hub CSPM genera un singolo risultato per ogni controllo, anche se il controllo si applica a più di uno standard. Se non attivi i risultati

del controllo consolidato, Security Hub CSPM genera un risultato separato per ogni standard abilitato a cui si applica un controllo. Ad esempio, se si abilitano due standard e un controllo si applica a entrambi, si ottengono due risultati distinti per il controllo, uno per ogni standard. Se si abilitano i risultati del controllo consolidato, si riceve un solo risultato per il controllo. Per ulteriori informazioni, consulta Risultati di controllo consolidati.

Riferimento dettagliato per standard

- AWS Standard di best practice di sicurezza di base in Security Hub CSPM
- Standard delle migliori pratiche di sicurezza AI nel Security Hub CSPM
- AWS Standard di etichettatura delle risorse in Security Hub CSPM
- CIS AWS Benchmark dei fondamenti nel Security Hub CSPM
- NIST SP 800-53 Revisione 5 nel Security Hub CSPM
- NIST SP 800-171 Revisione 2 nel Security Hub CSPM
- PCI DSS nel Security Hub CSPM
- Profilo CRI v2.2 nel Security Hub CSPM
- Service-managed standard nel Security Hub CSPM

AWS Standard di best practice di sicurezza di base in Security Hub CSPM

Sviluppato da AWS professionisti del settore, lo standard AWS Foundational Security Best Practices (FSBP) è una raccolta di best practice di sicurezza per le organizzazioni, indipendentemente dal settore o dalle dimensioni dell'organizzazione. Fornisce una serie di controlli che rilevano quando Account AWS e le risorse si discostano dalle migliori pratiche di sicurezza. Fornisce inoltre indicazioni prescrittive su come migliorare e mantenere il livello di sicurezza dell'organizzazione.

In AWS Security Hub CSPM, lo standard AWS Foundational Security Best Practices include controlli che valutano continuamente i tuoi carichi di lavoro Account AWS e ti aiutano a identificare le aree che si discostano dalle migliori pratiche di sicurezza. I controlli includono le migliori pratiche di sicurezza per risorse provenienti da più fonti. Servizi AWS A ogni controllo viene assegnata una categoria che riflette la funzione di sicurezza a cui si applica il controllo. Per un elenco di categorie e dettagli aggiuntivi, vedereCategorie di controllo.

Controlli che si applicano allo standard

L'elenco seguente specifica quali controlli CSPM AWS di Security Hub si applicano allo standard AWS Foundational Security Best Practices (v1.0.0). Per esaminare i dettagli di un controllo, scegli il controllo.

[Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS

[ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato

[ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit

[APIGateway.1] API Gateway REST e la registrazione dell'esecuzione dell' WebSocket API devono essere abilitati

[APIGateway.2] Le fasi API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend

[APIGateway.3] Le fasi API REST di API Gateway dovrebbero avere AWS X-Ray tracciamento abilitato

[APIGateway.4] API Gateway deve essere associato a un ACL Web WAF

[APIGateway.5] I dati della cache dell'API REST di API Gateway devono essere crittografati quando sono inattivi

[APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione

[APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages

[APIGateway.10] Le integrazioni API Gateway V2 devono utilizzare HTTPS per le connessioni private

[APIGateway.11] I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate

[AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata

[AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API

[Athena.4] I gruppi di lavoro Athena dovrebbero avere la registrazione abilitata

[AutoScaling.1] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB

[AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità

[AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)

[Autoscaling.5] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici

[AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità

[AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2

[Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi

[BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC

[BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata

[BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica

[BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata

[CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata

[CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati

[CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato

[CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito

[CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato

[CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata

[CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato

[CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS

[CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS

[CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate

[CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate

[CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti

[CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine

[CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata

[CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda

[CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati

[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura

[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata

[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs

[CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili

[CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato

[CodeBuild.3] I log CodeBuild S3 devono essere crittografati

[CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]

[CodeBuild.7] le esportazioni dei gruppi di CodeBuild report devono essere crittografate quando sono inattive

[Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate

[Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate

[Cognito.4] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata

[Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito

[Cognito.6] I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata

[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse

[Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata

[DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi

[DataSync.1] DataSync le attività dovrebbero avere la registrazione abilitata

[DMS.1] Le istanze di replica del Database Migration Service non devono essere pubbliche

[DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato

[DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata

[DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata

[DMS.9] Gli endpoint DMS devono utilizzare SSL

[DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata

[DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato

[DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato

[DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità

[DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi

[DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato

[DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche

[DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch

[DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata

[DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito

[DynamoDB.1] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda

[DynamoDB.2] Le tabelle DynamoDB dovrebbero avere il ripristino point-in-time abilitato

[DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi

[DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata

[DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito

[EC2.1] Le istantanee di Amazon EBS non devono essere configurate per essere ripristinabili pubblicamente

[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita

[EC2.3] I volumi Amazon EBS collegati devono essere crittografati quando sono inattivi

[EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato

[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC

[EC2.7] La crittografia predefinita di EBS deve essere abilitata

[EC2.8] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)

[EC2.9] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico

[EC2.10] Amazon EC2 deve essere configurato per utilizzare gli endpoint VPC creati per il servizio Amazon EC2

[EC2.15] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici

[EC2.16] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse

[EC2.17] Le istanze Amazon EC2 non devono utilizzare più ENI

[EC2.18] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate

[EC2.19] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio

[EC2.20] Entrambi i tunnel VPN per un AWS Site-to-Site La connessione VPN dovrebbe essere attiva

[EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389

[EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC

[EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati

[EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete

[EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata

[EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR

[EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry

[EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager

[EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts

[EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager

[EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)

[EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata

[EC2.172] Le impostazioni VPC Block Public Access di EC2 dovrebbero bloccare il traffico del gateway Internet

[EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati

[EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination

[EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati

[EC2.182] Le impostazioni di blocco dell'accesso pubblico devono essere abilitate per gli snapshot di Amazon EBS

[EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2

[ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata

[ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag

[ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata

[ECS.2] Ai servizi ECS non dovrebbero essere assegnati automaticamente indirizzi IP pubblici

[ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host

[ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati

[ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root

[ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore

[ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione

[ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate

[ECS.12] I cluster ECS devono utilizzare Container Insights

[ECS.16] I set di attività ECS non devono assegnare automaticamente indirizzi IP pubblici

[ECS.18] Le definizioni delle attività ECS devono utilizzare la crittografia in transito per i volumi EFS

[ECS.19] I provider di capacità ECS dovrebbero avere abilitato la protezione gestita dalle terminazioni

[ECS.20] Le definizioni delle attività ECS devono configurare gli utenti non root nelle definizioni dei container Linux

[ECS.21] Le definizioni delle attività ECS devono configurare gli utenti non amministratori nelle definizioni dei contenitori Windows

[EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS

[EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup

[EFS.3] I punti di accesso EFS devono applicare una directory principale

[EFS.4] I punti di accesso EFS devono applicare un'identità utente

[EFS.7] I file system EFS devono avere i backup automatici abilitati

[EFS.8] I file system EFS devono essere crittografati quando sono inattivi

[EKS.1] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico

[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata

[EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata

[EKS.9] I gruppi di nodi EKS devono essere eseguiti su una versione di Kubernetes supportata

I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati

[ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati

[ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato

[ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi

[ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito

[ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato

[ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito

[ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata

[ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati

[ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch

[ELB.1] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS

[ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager

[ELB.3] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS

[ELB.4] Application Load Balancer deve essere configurato per eliminare le intestazioni http non valide

[ELB.5] La registrazione di Application e Classic Load Balancers deve essere abilitata

[ELB.6] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata

[ELB.7] I Classic Load Balancer dovrebbero avere abilitato il drenaggio della connessione

[ELB.8] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita che sia solida AWS Config Durata

[ELB.9] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato

[ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità

[ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa

[ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità

[ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa

[ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate

[ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito

[ELB.21] I gruppi target di Application e Network Load Balancer devono utilizzare protocolli di controllo dello stato crittografati

[ELB.22] I gruppi target ELB devono utilizzare protocolli di trasporto crittografati

[EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici

[EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata

[EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo

[EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito

[ES.1] I domini Elasticsearch devono avere la crittografia a riposo abilitata

[ES.2] I domini Elasticsearch non devono essere accessibili al pubblico

[ES.3] I domini Elasticsearch devono crittografare i dati inviati tra i nodi

[ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch

[ES.5] I domini Elasticsearch devono avere la registrazione di controllo abilitata

[ES.6] I domini Elasticsearch devono avere almeno tre nodi di dati

[ES.7] I domini Elasticsearch devono essere configurati con almeno tre nodi master dedicati

[ES.8] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS

[EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata

[FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi

[FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup

[FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ

[FSx.4] I file system FSx for NetApp ONTAP devono essere configurati per l'implementazione Multi-AZ

[FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione

[Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate

[Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue

[GuardDuty.1] GuardDuty dovrebbe essere abilitato

[GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato

[GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata

[GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato

[GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata

[GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata

[GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata

[GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato

[GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato

[GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato

[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi

[IAM.2] Gli utenti IAM non devono avere policy IAM allegate

[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno

[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere

[IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console

[IAM.6] La MFA hardware deve essere abilitata per l'utente root

[IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide

[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse

[IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi

[Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata

[Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata

[Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata

[Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata

[Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi

[Kinesis.3] I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato

[KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS

[KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS

[KMS.3] AWS KMS keys non devono essere eliminati involontariamente

[KMS.5] Le chiavi KMS non devono essere accessibili al pubblico

[Lambda.1] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico

[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati

[Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità

[Macie.1] Amazon Macie dovrebbe essere abilitato

[Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato

[MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch

[MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker

[MSK.3] I connettori MSK Connect devono essere crittografati in transito

[MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato

[MSK.5] I connettori MSK devono avere la registrazione abilitata

[MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato

[Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi

[Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch

[Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche

[Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata

[Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati

[Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive

[Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata

[Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee

[NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata

[NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato

[NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi

[NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati

[NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto

[NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata

[NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata

[Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata

[Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico

[Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi

[Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch

[Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata

[Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati

[Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato

[Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente

[Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software

[PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata

[Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS

[RDS.1] L'istantanea RDS deve essere privata

[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible

[RDS.3] Le istanze DB RDS devono avere la crittografia a riposo abilitata

[RDS.4] Gli snapshot del cluster RDS e gli snapshot del database devono essere crittografati quando sono inattivi

[RDS.5] Le istanze DB RDS devono essere configurate con più zone di disponibilità

[RDS.6] Il monitoraggio avanzato deve essere configurato per le istanze DB RDS

[RDS.7] I cluster RDS devono avere la protezione da eliminazione abilitata

[RDS.8] Le istanze DB RDS devono avere la protezione da eliminazione abilitata

[RDS.9] Le istanze DB RDS devono pubblicare i log in Logs CloudWatch

[RDS.10] L'autenticazione IAM deve essere configurata per le istanze RDS

[RDS.11] Le istanze RDS devono avere i backup automatici abilitati

[RDS.12] L'autenticazione IAM deve essere configurata per i cluster RDS

[RDS.13] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati

[RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato

[RDS.15] I cluster RDS DB devono essere configurati per più zone di disponibilità

[RDS.16] I cluster Aurora DB devono essere configurati per copiare i tag nelle istantanee DB

[RDS.17] Le istanze DB RDS devono essere configurate per copiare i tag negli snapshot

[RDS.19] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici del cluster

[RDS.20] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici delle istanze di database

[RDS.21] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database

[RDS.22] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database

[RDS.23] Le istanze RDS non devono utilizzare una porta predefinita del motore di database

[RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato

[RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato

[RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi

[RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch

[] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato

[RDS.36] Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch

[RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch

[RDS.40] Le istanze DB di RDS per SQL Server devono pubblicare i log in Logs CloudWatch

[RDS.41] Le istanze DB di RDS per SQL Server devono essere crittografate in transito

[RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch

[] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43

[RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito

[RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata

[RDS.46] Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso gateway Internet

[RDS.47] I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB

[RDS.48] I cluster RDS per MySQL DB devono essere configurati per copiare i tag nelle istantanee del DB

[RDS.50] I cluster RDS DB devono avere un periodo di conservazione dei backup sufficiente

[RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata

[Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico

[Redshift.2] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito

[Redshift.3] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate

[Redshift.4] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata

[Redshift.6] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati

[Redshift.7] I cluster Redshift devono utilizzare un routing VPC avanzato

[Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito

[Redshift.10] I cluster Redshift devono essere crittografati a riposo

[Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate

[Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ

[RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato

[RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL

[RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico

[RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito

[RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch

[S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate

[S3.2] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura

[S3.3] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura

[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS

[S3.6] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS

[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico

[S3.9] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata

[S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3

[S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita

[S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate

[S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate

[S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita

[SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet

[SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato

[SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook

[SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1

[SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato

[SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate

[SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container

[SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container

[SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato

[SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato

[SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata

[SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato

[SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container

[SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari

[SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys

[SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore

[SecretsManager.1] I segreti di Secrets Manager devono avere la rotazione automatica abilitata

[SecretsManager.2] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente

[SecretsManager.3] Rimuovi i segreti inutilizzati di Secrets Manager

[SecretsManager.4] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni

[ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione

[SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail

[SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico

[SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive

[SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico

[SSM.1] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager

[SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch

[SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT

[SSM.4] I documenti SSM non devono essere pubblici

[SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch

[SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata

[StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata

[Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint

[Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata

[WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata

[WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione

[WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola

[WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole

[WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione

[WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola

[WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

[WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole

[WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch

[WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi

[WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Standard delle migliori pratiche di sicurezza AI nel Security Hub CSPM

Lo standard AI Security Best Practices è un insieme di controlli di sicurezza automatizzati che rilevano quando le risorse AI distribuite non sono in linea con le migliori pratiche di sicurezza. Sviluppato da esperti AWS di sicurezza, questo standard fornisce un set curato di controlli che consentono di identificare le aree in cui i carichi di lavoro di intelligenza artificiale si discostano dalle configurazioni di sicurezza consigliate.

In AWS Security Hub CSPM, lo standard AI Security Best Practices include controlli che valutano continuamente le tue risorse. I controlli riguardano i domini di sicurezza tra cui, a titolo esemplificativo ma non esaustivo, l'isolamento della rete, la crittografia a riposo e in transito, il posizionamento dei VPC AWS KMS , l'utilizzo delle chiavi e i requisiti del registro privato. A ogni controllo viene assegnata una categoria che riflette la funzione di sicurezza a cui si applica il controllo. Per un elenco di categorie e dettagli aggiuntivi, vedereCategorie di controllo in Security Hub CSPM.

Lo standard AI Security Best Practices ha il seguente Amazon Resource Name (ARN):`arn:aws:securityhub:`*`region`*`::standards/ai-security-best-practices/v/1.0.0`, dove si *`region`* trova il codice regionale applicabile. Regione AWS Puoi anche utilizzare il GetEnabledStandardsfunzionamento dell'API CSPM Security Hub per recuperare l'ARN di uno standard attualmente abilitato.

Controlli che si applicano allo standard

L'elenco seguente specifica quali controlli CSPM AWS di Security Hub si applicano allo standard AI Security Best Practices (v1.0.0). Per esaminare i dettagli di un controllo, scegli il controllo.

- [Bedrock.1] Le fonti di dati Amazon Bedrock devono essere crittografate e gestite dai clienti AWS KMS keys
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys

- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [BedrockAgentCore.7] Gli interpreti di codice AgentCore personalizzato Bedrock devono utilizzare una configurazione di rete privata
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari

- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SageMaker.20] le definizioni dei lavori di spiegabilità dei SageMaker modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.21] le istanze di SageMaker notebook devono essere crittografate e gestite dal cliente AWS KMS keys
- [SageMaker.22] le pianificazioni di SageMaker monitoraggio dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.23] gli esperimenti di SageMaker inferenza dovrebbero avere il volume di archiviazione delle istanze crittografato e gestito dal cliente AWS KMS keys
- [SageMaker.24] gli esperimenti di SageMaker inferenza dovrebbero avere l'archiviazione dei dati crittografata e gestita dal cliente AWS KMS keys
- [SageMaker.25] le definizioni dei lavori di qualità SageMaker del modello dovrebbero avere l'isolamento della rete abilitato

AWS Standard di etichettatura delle risorse in Security Hub CSPM

Lo standard AWS Resource Tagging, sviluppato da AWS Security Hub CSPM, ti aiuta a determinare se nelle tue AWS risorse mancano dei tag. I tag sono coppie chiave-valore che fungono da metadati per l'organizzazione delle risorse. AWS Con la maggior parte AWS delle risorse, è possibile aggiungere tag a una risorsa al momento della creazione della risorsa o dopo averla creata. Esempi di risorse includono CloudFront distribuzioni Amazon, istanze Amazon Elastic Compute Cloud (Amazon EC2) e segreti in. AWS Secrets Manager I tag possono aiutarti a gestire, identificare, organizzare, cercare e filtrare le risorse. AWS

Ogni tag è costituito da due parti:

- Una chiave di tag, ad esempio `CostCenter`, `Environment`, o. `Project` Le chiavi tag distinguono tra maiuscole e minuscole.
- Un valore di tag, ad esempio o. `111122223333` `Production` Come le chiavi dei tag, i valori dei tag distinguono tra maiuscole e minuscole.

È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Per informazioni sull'aggiunta di tag alle AWS risorse, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

Per ogni controllo che si applica allo standard AWS Resource Tagging in Security Hub CSPM, puoi opzionalmente utilizzare il parametro supported per specificare le chiavi dei tag che desideri vengano controllate dal controllo. Se non specificate alcuna chiave di tag, il controllo verifica solo l'esistenza di almeno una chiave di tag e fallisce se una risorsa non ha alcuna chiave di tag.

Prima di abilitare lo standard AWS Resource Tagging, è importante abilitare e configurare la registrazione delle risorse in AWS Config. Quando configurate la registrazione delle risorse, assicuratevi anche di abilitarla per tutti i tipi di AWS risorse controllate dai controlli che si applicano allo standard. In caso contrario, Security Hub CSPM potrebbe non essere in grado di valutare le risorse appropriate e generare risultati accurati per i controlli che si applicano allo standard. Per ulteriori informazioni, incluso un elenco dei tipi di risorse da registrare, vedere. AWS Config Risorse necessarie per i risultati del controllo

Dopo aver abilitato lo standard AWS Resource Tagging, iniziate a ricevere i risultati dei controlli che si applicano allo standard. Tieni presente che possono essere necessarie fino a 18 ore prima che Security Hub CSPM generi risultati per i controlli che utilizzano la stessa regola AWS Config collegata ai servizi dei controlli che si applicano ad altri standard abilitati. Per ulteriori informazioni, consulta Pianificazione dell'esecuzione dei controlli di sicurezza.

Lo standard AWS Resource Tagging ha il seguente Amazon Resource Name (ARN)`arn:aws:securityhub:`*`region`*`::standards/aws-resource-tagging-standard/v/1.0.0`:, *`region`* dove si trova il codice regionale applicabile. Regione AWS Puoi anche utilizzare il GetEnabledStandardsfunzionamento dell'API CSPM Security Hub per recuperare l'ARN di uno standard attualmente abilitato.

> **Note**
>
> Lo standard AWS Resource Tagging non è disponibile nelle regioni Asia Pacifico (Nuova Zelanda) e Asia Pacifico (Taipei).

Controlli che si applicano allo standard

L'elenco seguente specifica quali controlli CSPM AWS di Security Hub si applicano allo standard AWS Resource Tagging (v1.0.0). Per esaminare i dettagli di un controllo, scegli il controllo.

- [ACM.3] I certificati ACM devono essere etichettati
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [AppSync.4] AWS AppSync Le API GraphQL devono essere etichettate
- [Athena.2] I cataloghi di dati Athena devono essere etichettati
- [Athena.3] I gruppi di lavoro Athena devono essere etichettati
- [AutoScaling.10] I gruppi EC2 Auto Scaling devono essere etichettati
- [Backup.2] AWS Backup i punti di ripristino devono essere etichettati
- [Backup.3] AWS Backup i vault devono essere etichettati
- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [Backup.5] AWS Backup i piani di backup devono essere etichettati
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.2] Le politiche di pianificazione dei batch devono essere etichettate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [CloudFormation.2] gli CloudFormation stack devono essere etichettati
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [] CloudTrail.9 i trail devono essere etichettati CloudTrail
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate

- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [DataSync.2] le DataSync attività devono essere etichettate
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DynamoDB.5] Le tabelle DynamoDB devono essere etichettate
- [EC2.33] Gli allegati del gateway di transito EC2 devono essere etichettati
- [EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate
- [EC2.35] Le interfacce di rete EC2 devono essere etichettate
- [EC2.36] I gateway per i clienti EC2 devono essere etichettati
- [EC2.37] Gli indirizzi IP elastici EC2 devono essere etichettati
- [EC2.38] Le istanze EC2 devono essere etichettate
- [EC2.39] I gateway Internet EC2 devono essere etichettati
- [EC2.40] I gateway NAT EC2 devono essere etichettati
- [EC2.41] Gli ACL di rete EC2 devono essere etichettati
- [EC2.42] Le tabelle delle rotte EC2 devono essere etichettate
- [EC2.43] I gruppi di sicurezza EC2 devono essere etichettati
- [EC2.44] Le sottoreti EC2 devono essere etichettate
- [EC2.45] I volumi EC2 devono essere etichettati
- [EC2.46] I VPC Amazon devono essere etichettati
- [EC2.47] I servizi endpoint Amazon VPC devono essere etichettati
- [EC2.48] I log di flusso di Amazon VPC devono essere etichettati
- [EC2.49] Le connessioni peering Amazon VPC devono essere etichettate
- [EC2.50] I gateway VPN EC2 devono essere etichettati
- [EC2.52] I gateway di transito EC2 devono essere etichettati
- [EC2.174] I set di opzioni DHCP EC2 devono essere etichettati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati

- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ECS.13] I servizi ECS devono essere etichettati
- [ECS.14] I cluster ECS devono essere etichettati
- [ECS.15] Le definizioni delle attività ECS devono essere contrassegnate
- [EFS.5] I punti di accesso EFS devono essere etichettati
- [EKS.6] I cluster EKS devono essere etichettati
- [EKS.7] Le configurazioni dei provider di identità EKS devono essere contrassegnate
- [ES.9] I domini Elasticsearch devono essere etichettati
- [EventBridge.2] i bus EventBridge degli eventi devono essere etichettati
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.1] AWS Glue i lavori devono essere etichettati
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [GuardDuty.3] Gli GuardDuty IPSets devono essere etichettati
- [GuardDuty.4] i GuardDuty rilevatori devono essere etichettati
- [IAM.23] Gli analizzatori IAM Access Analyzer devono essere etichettati
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate

- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.2] Gli stream Kinesis devono essere etichettati
- [Lambda.6] Le funzioni Lambda devono essere etichettate
- [MQ.4] I broker Amazon MQ devono essere etichettati
- [NetworkFirewall.7] I firewall Network Firewall devono essere etichettati
- [NetworkFirewall.8] Le politiche firewall di Network Firewall devono essere etichettate
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [PCA.2] AWS Le autorità di certificazione CA private devono essere contrassegnate
- [RDS.28] I cluster RDS DB devono essere etichettati
- [RDS.29] Gli snapshot del cluster RDS DB devono essere etichettati
- [RDS.30] Le istanze DB RDS devono essere etichettate
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RDS.32] Gli snapshot RDS DB devono essere etichettati
- [RDS.33] I gruppi di sottoreti RDS DB devono essere etichettati
- [Redshift.11] I cluster Redshift devono essere etichettati

- [Redshift.12] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate
- [Redshift.13] Le istantanee del cluster Redshift devono essere etichettate
- [Redshift.14] I gruppi di sottoreti del cluster Redshift devono essere etichettati
- [Redshift.17] I gruppi di parametri del cluster Redshift devono essere etichettati
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SecretsManager.5] I segreti di Secrets Manager devono essere etichettati
- [SES.1] Gli elenchi di contatti SES devono essere etichettati
- [SES.2] I set di configurazione SES devono essere etichettati
- [SNS.3] Gli argomenti SNS devono essere etichettati
- [] Le code SQS devono essere etichettate SQS.2
- [SSM.5] I documenti SSM devono essere etichettati
- [StepFunctions.2] Le attività di Step Functions devono essere etichettate
- [Transfer.1] AWS Transfer Family i flussi di lavoro devono essere etichettati
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [Transfer.5] I certificati Transfer Family devono essere etichettati
- [Transfer.6] I connettori Transfer Family devono essere etichettati
- [Transfer.7] I profili Transfer Family devono essere etichettati

CIS AWS Benchmark dei fondamenti nel Security Hub CSPM

Il benchmark Center for Internet Security (CIS) AWS Foundations funge da set di best practice per la configurazione della sicurezza per. AWS Queste best practice accettate dal settore forniscono procedure di implementazione e valutazione chiare e dettagliate. Dai sistemi operativi ai servizi cloud e ai dispositivi di rete, i controlli di questo benchmark aiutano a proteggere i sistemi specifici utilizzati dall'organizzazione.

AWS Security Hub CSPM supporta le versioni CIS AWS Foundations Benchmark 5.0.0, 3.0.0, 1.4.0 e 1.2.0. Questa pagina elenca i controlli di sicurezza supportati da ciascuna versione. Fornisce inoltre un confronto tra le versioni.

CIS AWS Foundations Benchmark versione 5.0.0

Security Hub CSPM supporta la versione 5.0.0 (v5.0.0) del benchmark CIS Foundations. AWS Security Hub CSPM ha soddisfatto i requisiti della certificazione del software di sicurezza CIS e ha ottenuto la certificazione del software di sicurezza CIS per i seguenti benchmark CIS:

- Benchmark CIS per CIS AWS Foundations Benchmark, v5.0.0, livello 1
- Benchmark CIS per CIS AWS Foundations Benchmark, v5.0.0, livello 2

Controlli che si applicano al CIS AWS Foundations Benchmark versione 5.0.0

[Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS

[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura

[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata

[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail

[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse

[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita

[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC

[EC2.7] La crittografia predefinita di EBS deve essere abilitata

[EC2.8] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)

[EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389

[EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto

[EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server

[EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS

[EFS.8] I file system EFS devono essere crittografati quando sono inattivi

[IAM.2] Gli utenti IAM non devono avere policy IAM allegate

[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno

[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere

[IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console

[IAM.6] La MFA hardware deve essere abilitata per l'utente root

[IAM.9] L'MFA deve essere abilitata per l'utente root

[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14

[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password

[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS

[IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse

[IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi

[IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata

[IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato

[KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata

[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible

[RDS.3] Le istanze DB RDS devono avere la crittografia a riposo abilitata

[RDS.5] Le istanze DB RDS devono essere configurate con più zone di disponibilità

[RDS.13] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati

[RDS.15] I cluster RDS DB devono essere configurati per più zone di disponibilità

[S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate

[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS

[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico

[S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata

[S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto

[S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto

CIS AWS Foundations Benchmark versione 3.0.0

Security Hub CSPM supporta la versione 3.0.0 (v3.0.0) del benchmark CIS Foundations. AWS Security Hub CSPM ha soddisfatto i requisiti della certificazione del software di sicurezza CIS e ha ottenuto la certificazione del software di sicurezza CIS per i seguenti benchmark CIS:

- Benchmark CIS per CIS AWS Foundations Benchmark, v3.0.0, livello 1
- Benchmark CIS per CIS AWS Foundations Benchmark, v3.0.0, livello 2

Controlli che si applicano al CIS AWS Foundations Benchmark versione 3.0.0

[Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS

[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura

[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata

[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail

[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse

[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita

[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC

[EC2.7] La crittografia predefinita di EBS deve essere abilitata

[EC2.8] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)

[EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389

[EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto

[EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server

[EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS

[IAM.2] Gli utenti IAM non devono avere policy IAM allegate

[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno

[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere

[IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console

[IAM.6] La MFA hardware deve essere abilitata per l'utente root

[IAM.9] L'MFA deve essere abilitata per l'utente root

[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14

[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password

[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS

[IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse

[IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi

[IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata

[IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato

[KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata

[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible

[RDS.3] Le istanze DB RDS devono avere la crittografia a riposo abilitata

[RDS.13] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati

[S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate

[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS

[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico

[S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata

[S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto

[S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto

CIS AWS Foundations Benchmark versione 1.4.0

Security Hub CSPM supporta la versione 1.4.0 (v1.4.0) del benchmark CIS Foundations. AWS

Controlli che si applicano al CIS AWS Foundations Benchmark versione 1.4.0

[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura

[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata

[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs

[CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico

[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail

[CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»

[CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM

[CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrail alla configurazione

[CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per Console di gestione AWS errori di autenticazione

[CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione pianificata delle chiavi gestite dal cliente

[CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3

[CloudWatch.9] Assicurati che esistano un filtro metrico di registro e un allarme per AWS Config modifiche alla configurazione

[CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza

[CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)

[CloudWatch.12] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gateway di rete

[CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte

[CloudWatch.14] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche al VPC

[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse

[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita

[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC

[EC2.7] La crittografia predefinita di EBS deve essere abilitata

[EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389

[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi

[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno

[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere

[IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console

[IAM.6] La MFA hardware deve essere abilitata per l'utente root

[IAM.9] L'MFA deve essere abilitata per l'utente root

[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14

[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password

[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS

[IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse

[KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata

[RDS.3] Le istanze DB RDS devono avere la crittografia a riposo abilitata

[S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate

[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS

[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico

[S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata

CIS AWS Foundations Benchmark versione 1.2.0

Security Hub CSPM supporta la versione 1.2.0 (v1.2.0) del benchmark CIS Foundations. AWS Security Hub CSPM ha soddisfatto i requisiti della certificazione del software di sicurezza CIS e ha ottenuto la certificazione del software di sicurezza CIS per i seguenti benchmark CIS:

- Benchmark CIS per CIS AWS Foundations Benchmark, v1.2.0, livello 1
- Benchmark CIS per CIS AWS Foundations Benchmark, v1.2.0, livello 2

Controlli che si applicano al CIS AWS Foundations Benchmark versione 1.2.0

[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura

[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata

[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs

[CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico

[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail

[CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»

[CloudWatch.2] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate

[CloudWatch.3] Assicurati che esistano un filtro metrico di registro e un allarme per l'accesso alla console di gestione senza MFA

[CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM

[CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrail alla configurazione

[CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per Console di gestione AWS errori di autenticazione

[CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione pianificata delle chiavi gestite dal cliente

[CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3

[CloudWatch.9] Assicurati che esistano un filtro metrico di registro e un allarme per AWS Config modifiche alla configurazione

[CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza

[CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)

[CloudWatch.12] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gateway di rete

[CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte

[CloudWatch.14] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche al VPC

[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse

[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita

[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC

[EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22

[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389

[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi

[IAM.2] Gli utenti IAM non devono avere policy IAM allegate

[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno

[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere

[IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console

[IAM.6] La MFA hardware deve essere abilitata per l'utente root

[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse

[IAM.9] L'MFA deve essere abilitata per l'utente root

[IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola

[IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola

[IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo

[IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero

[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14

[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password

[IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno

[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS

[KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata

Confronto delle versioni per CIS AWS Foundations Benchmark

Questa sezione riassume le differenze tra le versioni specifiche del benchmark Center for Internet Security (CIS AWS) Foundations: v5.0.0, v3.0.0, v1.4.0 e v1.2.0. AWS Security Hub CSPM supporta ognuna di queste versioni del benchmark AWS CIS Foundations. Tuttavia, consigliamo di utilizzare la versione 5.0.0 per rimanere aggiornati sulle migliori pratiche di sicurezza. È possibile abilitare più versioni degli standard CIS AWS Foundations Benchmark contemporaneamente. Per informazioni sull'abilitazione degli standard, vedere. Abilitazione di uno standard di sicurezza Se desideri eseguire l'aggiornamento alla versione 5.0.0, abilitalo prima di disabilitare una versione precedente. In questo modo si evitano lacune nei controlli di sicurezza. Se utilizzi l'integrazione CSPM di Security Hub con

AWS Organizations e desideri abilitare in batch la v5.0.0 in più account, ti consigliamo di utilizzare la configurazione centrale.

Mappatura dei controlli in base ai requisiti CIS in ogni versione

Scopri quali controlli supporta ogni versione di CIS AWS Foundations Benchmark.

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS	1.2	1.2	1.2	1.18
[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura	3.1	3.1	3.1	2.1
[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata	3.5	3.5	3.7	2.7
[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata	3.2	3.2	3.2	2.2
[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	3.4	2.4
[CloudTrail.6] Assicurati che il bucket S3 utilizzato per	Non supportat	Non supportat	3.3	2.3

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
archiviare i CloudTrail log non sia accessibile al pubblico	o: il CIS ha rimosso questo requisito	o: il CIS ha rimosso questo requisito		
[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail	3.4	3.4	3.6	2.6
[CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»	Non supportato: controllo manuale	Non supportato: controllo manuale	4.3	3.3
[CloudWatch.2] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate	Non supportato: controllo manuale	Non supportato: controllo manuale	Non supportato: controllo manuale	3.1
[CloudWatch.3] Assicurati che esistano un filtro metrico di registro e un allarme per l'accesso alla console di gestione senza MFA	Non supportato: controllo manuale	Non supportato: controllo manuale	Non supportato: controllo manuale	3.2
[CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM	Non supportato: controllo manuale	Non supportato: controllo manuale	4.4	3.4

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrail alla configurazione	Non supportato: controllo manuale	Non supportato: controllo manuale	4.5	3.5
[CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per Console di gestione AWS errori di autenticazione	Non supportato: controllo manuale	Non supportato: controllo manuale	4.6	3.6
[CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione pianificata delle chiavi gestite dal cliente	Non supportato: controllo manuale	Non supportato: controllo manuale	4.7	3.7
[CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3	Non supportato: controllo manuale	Non supportato: controllo manuale	4.8	3.8
[CloudWatch.9] Assicurati che esistano un filtro metrico di registro e un allarme per AWS Config modifiche alla configurazione	Non supportato: controllo manuale	Non supportato: controllo manuale	4.9	3.9
[CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza	Non supportato: controllo manuale	Non supportato: controllo manuale	4.10	3,10

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)	Non supportato: controllo manuale	Non supportato: controllo manuale	4.11	3,11
[CloudWatch.12] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gateway di rete	Non supportato: controllo manuale	Non supportato: controllo manuale	4.12	3,12
[CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte	Non supportato: controllo manuale	Non supportato: controllo manuale	4.13	3.13
[CloudWatch.14] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche al VPC	Non supportato: controllo manuale	Non supportato: controllo manuale	4.14	3,14
[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse	3.3	3.3	3.5	2.5
[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita	5.5	5.4	5.3	4.3
[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC	3.7	3.7	3.9	2.9

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[EC2.7] La crittografia predefinita di EBS deve essere abilitata	5.1.1	2.2.1	2.2.1	Non supportata
[EC2.8] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)	5.7	5.6	Non supportata	Non supportata
[EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22	Non supportato: sostituito dai requisiti 5.3 e 5.4	Non supportato: sostituito dai requisiti 5.2 e 5.3	Non supportato: sostituito dai requisiti 5.2 e 5.3	4.1
[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389	Non supportato: sostituito dai requisiti 5.3 e 5.4	Non supportato: sostituito dai requisiti 5.2 e 5.3	Non supportato: sostituito dai requisiti 5.2 e 5.3	4.2
[EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389	5.2	5.1	5.1	Non supportata
[EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto	5.3	5.2	Non supportata	Non supportata

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server	5.4	5.3	Non supportata	Non supportata
[EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS	2.3.1	2.4.1	Non supportata	Non supportata
[EFS.8] I file system EFS devono essere crittografati quando sono inattivi	2.3.1	Non supportata	Non supportata	Non supportata
[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi	Non supportata	Non supportata	1.16	1,22
[IAM.2] Gli utenti IAM non devono avere policy IAM allegate	1.14	1.15	Non supportata	1.16
[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno	1.13	1.14	1.14	1.4
[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere	1.3	1.4	1.4	1.12

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console	1.9	1.10	1.10	1.2
[IAM.6] La MFA hardware deve essere abilitata per l'utente root	1.5	1.6	1.6	1.14
[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse	Non supportato, vedi invece [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse	Non supportato, vedi [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse invece	Non supportato, vedi [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse invece	1.3
[IAM.9] L'MFA deve essere abilitata per l'utente root	1.4	1.5	1.5	1.13
[IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1.5

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1.6
[IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1,7
[IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1.8
[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14	1,7	1.8	1.8	1.9
[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password	1.8	1.9	1.9	1.10

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1.11
[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS	1.16	1,17	1,17	1.2
[IAM.20] Evita l'uso dell'utente root	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1.1
[IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse	1.11	1.12	1.12	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi	1.18	1,19	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata	1.21	1,22	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato	1.19	1,20	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata	3.6	3.6	3.8	2.8

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[Macie.1] Amazon Macie dovrebbe essere abilitato	Non supportato: controllo manuale	Non supportato: controllo manuale	Non supportato: controllo manuale	Non supportato: controllo manuale
[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible	2.2.3	2.3.3	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[RDS.3] Le istanze DB RDS devono avere la crittografia a riposo abilitata	2.2.1	2.3.1	2.3.1	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[RDS.5] Le istanze DB RDS devono essere configurate con più zone di disponibilità	2.2.4	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[RDS.13] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati	2.2.2	2.3.2	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[RDS.15] I cluster RDS DB devono essere configurati per più zone di disponibilità	2.2.4	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate	2.1.4	2.1.4	2.1.5	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive

ID e titolo di controllo	Requisito CIS v5.0.0	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS	2.1.1	2.1.1	2.1.2	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico	2.1.4	2.1.4	2.1.5	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata	2.1.2	2.1.2	2.1.3	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive

ARN per CIS AWS Fondamenti e benchmark

Quando abiliti una o più versioni del benchmark CIS AWS Foundations, inizi a ricevere i risultati nel AWS Security Finding Format (ASFF). In ASFF, ogni versione utilizza il seguente Amazon Resource Name (ARN):

Benchmark CIS AWS Foundations v5.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/5.0.0
```

Benchmark CIS AWS Foundations v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/3.0.0
```

Benchmark CIS AWS Foundations v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/1.4.0
```

Benchmark CIS AWS Foundations v1.2.0

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

È possibile utilizzare il GetEnabledStandardsfunzionamento dell'API CSPM Security Hub per trovare l'ARN di uno standard abilitato.

I valori precedenti sono per. `StandardsArn` Tuttavia, `StandardsSubscriptionArn` si riferisce alla risorsa di abbonamento standard che Security Hub CSPM crea quando ci si abbona a uno standard chiamando una BatchEnableStandardsregione.

> **Note**
>
> Quando abiliti una versione del benchmark CIS AWS Foundations, possono essere necessarie fino a 18 ore prima che Security Hub CSPM generi risultati per i controlli che utilizzano la stessa regola AWS Config collegata ai servizi dei controlli abilitati in altri standard abilitati. Per ulteriori informazioni sulla pianificazione per la generazione dei risultati del controllo, vedere. Pianificazione dell'esecuzione dei controlli di sicurezza

I campi di ricerca sono diversi se si attivano i risultati di controllo consolidati. Per informazioni su queste differenze, vedereImpatto del consolidamento sui campi e sui valori ASFF. Per esempi di risultati di controllo, vedereEsempi di risultati di controllo.

Requisiti CIS non supportati in Security Hub CSPM

Come indicato nella tabella precedente, Security Hub CSPM non supporta tutti i requisiti CIS in ogni versione del benchmark CIS Foundations. AWS Molti dei requisiti non supportati possono essere valutati solo esaminando manualmente lo stato delle risorse. AWS

NIST SP 800-53 Revisione 5 nel Security Hub CSPM

La pubblicazione speciale NIST 800-53 Revisione 5 (NIST SP 800-53 Rev. 5) è un framework di sicurezza informatica e conformità sviluppato dal National Institute of Standards and Technology (NIST), un'agenzia che fa parte del. U.S Dipartimento del Commercio. Questo framework di conformità fornisce un catalogo di requisiti di sicurezza e privacy per proteggere la riservatezza, l'integrità e la disponibilità dei sistemi di informazione e delle risorse critiche. U.S. le agenzie governative federali e gli appaltatori devono rispettare questi requisiti per proteggere i propri sistemi e le proprie organizzazioni. Le organizzazioni private possono inoltre utilizzare volontariamente i requisiti come quadro guida per ridurre i rischi di sicurezza informatica. Per ulteriori informazioni sul framework e sui relativi requisiti, vedere NIST SP 800-53 Rev. 5 nel NIST Computer Security Resource Center.

AWS Security Hub CSPM fornisce controlli di sicurezza che supportano un sottoinsieme dei requisiti NIST SP 800-53 Revisione 5. I controlli eseguono controlli di sicurezza automatici per determinate risorse. Servizi AWS Per abilitare e gestire questi controlli, è possibile abilitare il framework NIST SP 800-53 Revision 5 come standard in Security Hub CSPM. Tieni presente che i controlli non supportano i requisiti NIST SP 800-53 Revisione 5 che richiedono controlli manuali.

A differenza di altri framework, il framework NIST SP 800-53 Revision 5 non è prescrittivo su come valutare i suoi requisiti. Invece, il framework fornisce delle linee guida. In Security Hub CSPM, lo standard e i controlli NIST SP 800-53 Revision 5 rappresentano la comprensione da parte del servizio di queste linee guida.

Argomenti

- Configurazione della registrazione delle risorse per i controlli che si applicano allo standard
- Determinare quali controlli si applicano allo standard

Configurazione della registrazione delle risorse per i controlli che si applicano allo standard

Per ottimizzare la copertura e l'accuratezza dei risultati, è importante abilitare e configurare la registrazione delle risorse AWS Config prima di abilitare lo standard NIST SP 800-53 Revisione 5 in Security Hub AWS CSPM. Quando configuri la registrazione delle risorse, assicurati anche di

abilitarla per tutti i tipi di AWS risorse controllate dai controlli che si applicano allo standard. Questo è principalmente per i controlli che hanno un tipo di pianificazione innescato dalla modifica. Tuttavia, alcuni controlli con un tipo di pianificazione periodica richiedono anche la registrazione delle risorse. Se la registrazione delle risorse non è abilitata o configurata correttamente, Security Hub CSPM potrebbe non essere in grado di valutare le risorse appropriate e generare risultati accurati per i controlli che si applicano allo standard.

Per informazioni su come Security Hub CSPM utilizza la registrazione delle risorse AWS Config, vedere. Attivazione e configurazione AWS Config per Security Hub CSPM Per informazioni sulla configurazione della registrazione delle risorse in AWS Config, vedere Lavorare con il registratore di configurazione nella Guida per gli sviluppatori.AWS Config

La tabella seguente specifica i tipi di risorse da registrare per i controlli che si applicano allo standard NIST SP 800-53 Revision 5 in Security Hub CSPM.

Servizio AWS	Tipi di risorse
Gateway Amazon API	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Bedrock 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`

Servizio AWS	Tipi di risorse
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`
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`

Servizio AWS	Tipi di risorse
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 (IAM)	`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`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
OpenSearch Servizio Amazon	`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`

Servizio AWS	Tipi di risorse
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`
Servizio di notifica semplice Amazon (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`
Amazon SageMaker AI	`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`

Determinare quali controlli si applicano allo standard

L'elenco seguente specifica i controlli che supportano i requisiti NIST SP 800-53 Revisione 5 e si applicano allo standard NIST SP 800-53 Revisione 5 in Security Hub CSPM. AWS Per informazioni dettagliate sui requisiti specifici supportati da un controllo, scegliete il controllo. Quindi, fai riferimento

al campo Requisiti correlati nei dettagli del controllo. Questo campo specifica ogni requisito NIST supportato dal controllo. Se il campo non specifica un particolare requisito NIST, il controllo non supporta il requisito.

- [Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato
- [APIGateway.1] API Gateway REST e la registrazione dell'esecuzione dell' WebSocket API devono essere abilitati
- [APIGateway.2] Le fasi API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend
- [APIGateway.3] Le fasi API REST di API Gateway dovrebbero avere AWS X-Ray tracciamento abilitato
- [APIGateway.4] API Gateway deve essere associato a un ACL Web WAF
- [APIGateway.5] I dati della cache dell'API REST di API Gateway devono essere crittografati quando sono inattivi
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [AutoScaling.1] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB
- [AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità
- [AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)
- [Autoscaling.5] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici
- [AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità
- [AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi

- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura
- [CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata
- [CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata
- [CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs
- [CloudTrail.10] I data store di eventi di CloudTrail Lake devono essere crittografati con Customer Managed AWS KMS keys
- [CloudWatch.15] gli CloudWatch allarmi dovrebbero avere azioni specificate configurate
- [CloudWatch.16] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato
- [CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate
- [CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili
- [CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato
- [CodeBuild.3] I log CodeBuild S3 devono essere crittografati

- [CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]
- [Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse
- [DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [DMS.1] Le istanze di replica del Database Migration Service non devono essere pubbliche
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DynamoDB.1] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda
- [DynamoDB.2] Le tabelle DynamoDB dovrebbero avere il ripristino point-in-time abilitato
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup
- [DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata

- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.1] Le istantanee di Amazon EBS non devono essere configurate per essere ripristinabili pubblicamente
- [EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita
- [EC2.3] I volumi Amazon EBS collegati devono essere crittografati quando sono inattivi
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC
- [EC2.7] La crittografia predefinita di EBS deve essere abilitata
- [EC2.8] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.9] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico
- [EC2.10] Amazon EC2 deve essere configurato per utilizzare gli endpoint VPC creati per il servizio Amazon EC2
- [EC2.12] Gli EIP Amazon EC2 non utilizzati devono essere rimossi
- [EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22
- [EC2.15] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici
- [EC2.16] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse
- [EC2.17] Le istanze Amazon EC2 non devono utilizzare più ENI
- [EC2.18] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate
- [EC2.19] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio
- [EC2.20] Entrambi i tunnel VPN per un AWS Site-to-Site La connessione VPN dovrebbe essere attiva
- [EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup

- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR
- [EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry
- [EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag
- [ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata
- [ECR.5] I repository ECR devono essere crittografati e gestiti dal cliente AWS KMS keys
- [ECS.2] Ai servizi ECS non dovrebbero essere assegnati automaticamente indirizzi IP pubblici
- [ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host
- [ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati
- [ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root
- [ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore
- [ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione
- [ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate
- [ECS.12] I cluster ECS devono utilizzare Container Insights
- [ECS.17] Le definizioni delle attività ECS non devono utilizzare la modalità di rete host
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio

- [EKS.1] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico
- [EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata
- [EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ELB.1] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [ELB.3] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS
- [ELB.4] Application Load Balancer deve essere configurato per eliminare le intestazioni http non valide
- [ELB.5] La registrazione di Application e Classic Load Balancers deve essere abilitata
- [ELB.6] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata
- [ELB.7] I Classic Load Balancer dovrebbero avere abilitato il drenaggio della connessione
- [ELB.8] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita che sia solida AWS Config Durata
- [ELB.9] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato
- [ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità

- [ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.16] Application Load Balancers deve essere associato a un AWS WAF ACL Web
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo
- [EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito
- [ES.1] I domini Elasticsearch devono avere la crittografia a riposo abilitata
- [ES.2] I domini Elasticsearch non devono essere accessibili al pubblico
- [ES.3] I domini Elasticsearch devono crittografare i dati inviati tra i nodi
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [ES.5] I domini Elasticsearch devono avere la registrazione di controllo abilitata
- [ES.6] I domini Elasticsearch devono avere almeno tre nodi di dati
- [ES.7] I domini Elasticsearch devono essere configurati con almeno tre nodi master dedicati
- [ES.8] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS
- [EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.1] GuardDuty dovrebbe essere abilitato

- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [KMS.3] AWS KMS keys non devono essere eliminati involontariamente
- [KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata
- [Lambda.1] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico
- [Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati
- [Lambda.3] Le funzioni Lambda devono trovarsi in un VPC
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker
- [MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby

- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato

- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata
- [RDS.1] L'istantanea RDS deve essere privata
- [RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible
- [RDS.3] Le istanze DB RDS devono avere la crittografia a riposo abilitata
- [RDS.4] Gli snapshot del cluster RDS e gli snapshot del database devono essere crittografati quando sono inattivi
- [RDS.5] Le istanze DB RDS devono essere configurate con più zone di disponibilità
- [RDS.6] Il monitoraggio avanzato deve essere configurato per le istanze DB RDS
- [RDS.7] I cluster RDS devono avere la protezione da eliminazione abilitata
- [RDS.8] Le istanze DB RDS devono avere la protezione da eliminazione abilitata
- [RDS.9] Le istanze DB RDS devono pubblicare i log in Logs CloudWatch
- [RDS.10] L'autenticazione IAM deve essere configurata per le istanze RDS
- [RDS.11] Le istanze RDS devono avere i backup automatici abilitati
- [RDS.12] L'autenticazione IAM deve essere configurata per i cluster RDS
- [RDS.13] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.15] I cluster RDS DB devono essere configurati per più zone di disponibilità
- [RDS.16] I cluster Aurora DB devono essere configurati per copiare i tag nelle istantanee DB
- [RDS.17] Le istanze DB RDS devono essere configurate per copiare i tag negli snapshot
- [RDS.19] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici del cluster
- [RDS.20] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici delle istanze di database
- [RDS.21] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database

- [RDS.22] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database
- [RDS.23] Le istanze RDS non devono utilizzare una porta predefinita del motore di database
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.26] Le istanze DB RDS devono essere protette da un piano di backup
- [RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.40] Le istanze DB di RDS per SQL Server devono pubblicare i log in Logs CloudWatch
- [RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico
- [Redshift.2] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito
- [Redshift.3] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate
- [Redshift.4] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata
- [Redshift.6] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati
- [Redshift.7] I cluster Redshift devono utilizzare un routing VPC avanzato
- [Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.2] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura
- [S3.3] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura

- [S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS
- [S3.6] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS
- [S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni
- [S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico
- [S3.9] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata
- [S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita
- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- [S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3
- [S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita
- S3.14[] I bucket S3 per uso generico devono avere il controllo delle versioni abilitato
- [S3.15] I bucket generici S3 devono avere Object Lock abilitato
- [S3.17] I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys
- [S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SecretsManager.1] I segreti di Secrets Manager devono avere la rotazione automatica abilitata
- [SecretsManager.2] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente
- [SecretsManager.3] Rimuovi i segreti inutilizzati di Secrets Manager
- [SecretsManager.4] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni

- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SNS.1] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [SSM.1] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager
- [SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch
- [SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT
- [SSM.4] I documenti SSM non devono essere pubblici
- [Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WAF.11] AWS WAF la registrazione ACL web deve essere abilitata
- [WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch

NIST SP 800-171 Revisione 2 nel Security Hub CSPM

La pubblicazione speciale NIST 800-171 Revisione 2 (NIST SP 800-171 Rev. 2) è un framework di sicurezza informatica e conformità sviluppato dal National Institute of Standards and Technology (NIST), un'agenzia che fa parte del. U.S Dipartimento del Commercio. Questo quadro di conformità fornisce i requisiti di sicurezza consigliati per proteggere la riservatezza delle informazioni controllate non classificate in sistemi e organizzazioni che non fanno parte del governo federale U.S. Le

informazioni non classificate controllate, note anche come CUI, sono informazioni sensibili che non soddisfano i criteri di classificazione governativi ma devono essere protette. Si tratta di informazioni considerate sensibili e create o possedute dal U.S governo federale o da altre entità per conto del governo federale U.S.

NIST SP 800-171 Rev. 2 fornisce i requisiti di sicurezza consigliati per proteggere la riservatezza del CUI quando:

- Le informazioni risiedono in sistemi e organizzazioni non federali,
- L'organizzazione non federale non raccoglie o conserva informazioni per conto di un'agenzia federale né utilizza o gestisce un sistema per conto di un'agenzia, e
- Non esistono requisiti di salvaguardia specifici per proteggere la riservatezza del CUI prescritti dalla legge, dai regolamenti o dalla politica governativa che autorizza la categoria CUI elencata nel registro CUI.

I requisiti si applicano a tutti i componenti dei sistemi e delle organizzazioni non federali che elaborano, archiviano o trasmettono i CUI o forniscono protezione di sicurezza per i componenti. Per ulteriori informazioni, vedere NIST SP 800-171 Rev. 2 nel NIST Computer Security Resource Center.

AWS Security Hub CSPM fornisce controlli di sicurezza che supportano un sottoinsieme dei requisiti NIST SP 800-171 Revisione 2. I controlli eseguono controlli di sicurezza automatici per determinate risorse. Servizi AWS Per abilitare e gestire questi controlli, è possibile abilitare il framework NIST SP 800-171 Revision 2 come standard in Security Hub CSPM. Tieni presente che i controlli non supportano i requisiti NIST SP 800-171 Revisione 2 che richiedono controlli manuali.

Argomenti

- Configurazione della registrazione delle risorse per i controlli che si applicano allo standard
- Determinare quali controlli si applicano allo standard

Configurazione della registrazione delle risorse per i controlli che si applicano allo standard

Per ottimizzare la copertura e l'accuratezza dei risultati, è importante abilitare e configurare la registrazione delle risorse AWS Config prima di abilitare lo standard NIST SP 800-171 Revision 2 in Security Hub AWS CSPM. Quando configuri la registrazione delle risorse, assicurati anche di abilitarla per tutti i tipi di AWS risorse controllate dai controlli che si applicano allo standard. In caso contrario, Security Hub CSPM potrebbe non essere in grado di valutare le risorse appropriate e generare risultati accurati per i controlli che si applicano allo standard.

Per informazioni su come Security Hub CSPM utilizza la registrazione delle risorse AWS Config, vedere. Attivazione e configurazione AWS Config per Security Hub CSPM Per informazioni sulla configurazione della registrazione delle risorse in AWS Config, vedere Lavorare con il registratore di configurazione nella Guida per gli sviluppatori.AWS Config

La tabella seguente specifica i tipi di risorse da registrare per i controlli che si applicano allo standard NIST SP 800-171 Revision 2 in Security Hub CSPM.

Servizio AWS	Tipi di risorse
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
Gateway Amazon API	`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(IAM)	`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`
Servizio Amazon Simple Storage (Amazon S3)	`AWS::S3::Bucket`
Servizio di notifica semplice di Amazon (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SSM)	`AWS::SSM::PatchCompliance`

Servizio AWS	Tipi di risorse
AWS WAF	`AWS::WAFv2::RuleGroup`

Determinare quali controlli si applicano allo standard

L'elenco seguente specifica i controlli che supportano i requisiti NIST SP 800-171 Revisione 2 e si applicano allo standard NIST SP 800-171 Revisione 2 in Security Hub CSPM. AWS Per informazioni dettagliate sui requisiti specifici supportati da un controllo, scegliete il controllo. Quindi, fai riferimento al campo Requisiti correlati nei dettagli del controllo. Questo campo specifica ogni requisito NIST supportato dal controllo. Se il campo non specifica un particolare requisito NIST, il controllo non supporta il requisito.

- [ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato
- [APIGateway.2] Le fasi API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata
- [CloudTrail.3] Almeno un CloudTrail percorso deve essere abilitato
- [CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata
- [CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»
- [CloudWatch.2] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate
- [CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM
- [CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrail alla configurazione
- [CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per Console di gestione AWS errori di autenticazione

- [CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione pianificata delle chiavi gestite dal cliente
- [CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3
- [CloudWatch.9] Assicurati che esistano un filtro metrico di registro e un allarme per AWS Config modifiche alla configurazione
- [CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza
- [CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)
- [CloudWatch.12] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gateway di rete
- [CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte
- [CloudWatch.14] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche al VPC
- [CloudWatch.15] gli CloudWatch allarmi dovrebbero avere azioni specificate configurate
- [EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC
- [EC2.10] Amazon EC2 deve essere configurato per utilizzare gli endpoint VPC creati per il servizio Amazon EC2
- [EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22
- [EC2.16] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse
- [EC2.18] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate
- [EC2.19] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio
- [EC2.20] Entrambi i tunnel VPN per un AWS Site-to-Site La connessione VPN dovrebbe essere attiva
- [EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata

- [EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [ELB.3] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS
- [ELB.8] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita che sia solida AWS Config Durata
- [GuardDuty.1] GuardDuty dovrebbe essere abilitato
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
- [IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
- [IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
- [IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
- [IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
- [IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto

- [S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS
- [S3.6] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS
- [S3.9] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata
- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- S3.14[] I bucket S3 per uso generico devono avere il controllo delle versioni abilitato
- [S3.17] I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys
- [SNS.1] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS
- [SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch
- [WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch

PCI DSS nel Security Hub CSPM

Il Payment Card Industry Data Security Standard (PCI DSS) è un framework di conformità di terze parti che fornisce una serie di regole e linee guida per la gestione sicura dei dati delle carte di credito e di debito. Il PCI Security Standards Council (SSC) crea e aggiorna questo framework.

AWS Security Hub CSPM fornisce uno standard PCI DSS che può aiutarti a rimanere conforme a questo framework di terze parti. È possibile utilizzare questo standard per scoprire le vulnerabilità di sicurezza nelle risorse che gestiscono i dati dei titolari di carta. AWS Si consiglia di abilitare questo standard in presenza di risorse Account AWS che archiviano, elaborano o trasmettono dati dei titolari di carta o dati di autenticazione sensibili. Le valutazioni del PCI SSC hanno convalidato questo standard.

Security Hub CSPM offre supporto sia per PCI DSS v3.2.1 che per PCI DSS v4.0.1. Ti consigliamo di utilizzare la versione 4.0.1 per rimanere aggiornato sulle migliori pratiche di sicurezza. Puoi avere entrambe le versioni dello standard abilitate contemporaneamente. Per informazioni sull'abilitazione degli standard, vedereAbilitazione di uno standard di sicurezza. Se attualmente utilizzi la versione 3.2.1 ma desideri utilizzare solo la versione 4.0.1, abilita la versione più recente prima di disabilitare la versione precedente. In questo modo si evitano lacune nei controlli di sicurezza. Se utilizzi l'integrazione CSPM di Security Hub con AWS Organizations e desideri abilitare in batch la v4.0.1 in più account, ti consigliamo di utilizzare la configurazione centrale per farlo.

Le seguenti sezioni specificano quali controlli si applicano a PCI DSS v3.2.1 e PCI DSS v4.0.1.

Controlli che si applicano a PCI DSS v3.2.1

L'elenco seguente specifica quali controlli CSPM di Security Hub si applicano a PCI DSS v3.2.1. Per esaminare i dettagli di un controllo, scegli il controllo.

[AutoScaling.1] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB

[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata

[CloudTrail.3] Almeno un CloudTrail percorso deve essere abilitato

[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs

[CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»

[CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili

[CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato

[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse

[DMS.1] Le istanze di replica del Database Migration Service non devono essere pubbliche

[EC2.1] Le istantanee di Amazon EBS non devono essere configurate per essere ripristinabili pubblicamente

[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita

[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC

[EC2.12] Gli EIP Amazon EC2 non utilizzati devono essere rimossi

[EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22

[ELB.1] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS

[ES.1] I domini Elasticsearch devono avere la crittografia a riposo abilitata

[ES.2] I domini Elasticsearch non devono essere accessibili al pubblico

[GuardDuty.1] GuardDuty dovrebbe essere abilitato

[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi

[IAM.2] Gli utenti IAM non devono avere policy IAM allegate

[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere

[IAM.6] La MFA hardware deve essere abilitata per l'utente root

[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse

[IAM.9] L'MFA deve essere abilitata per l'utente root

[IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide

[IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM

[KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata

[Lambda.1] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico

[Lambda.3] Le funzioni Lambda devono trovarsi in un VPC

[Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata

[Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico

[RDS.1] L'istantanea RDS deve essere privata

[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible

[Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico

[S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate

[S3.2] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura

[S3.3] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura

[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS

[S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni

[SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet

[SSM.1] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager

[SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch

[SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT

Controlli che si applicano a PCI DSS v4.0.1

L'elenco seguente specifica quali controlli CSPM di Security Hub si applicano a PCI DSS v4.0.1. Per esaminare i dettagli di un controllo, scegli il controllo.

[ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato

[ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit

[APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages

[AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata

[AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)

[Autoscaling.5] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici

[CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato

[CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate

[CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti

[CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito

[CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata

[CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato

[CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate

[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata

[CloudTrail.3] Almeno un CloudTrail percorso deve essere abilitato

[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

[CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico

[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail

[CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili

[CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato

[CodeBuild.3] I log CodeBuild S3 devono essere crittografati

[DMS.1] Le istanze di replica del Database Migration Service non devono essere pubbliche

[DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata

[DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato

[DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato

[DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato

[DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata

[DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata

[DMS.9] Gli endpoint DMS devono utilizzare SSL

[DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato

[DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche

[DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch

[DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito

[EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22

[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389

[EC2.15] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici

[EC2.16] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse

[EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)

[EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata

[EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389

[EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete

[EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata

[EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto

[EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server

[EC2.8] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)

[ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata

[ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate

[ECS.16] I set di attività ECS non devono assegnare automaticamente indirizzi IP pubblici

[ECS.2] Ai servizi ECS non dovrebbero essere assegnati automaticamente indirizzi IP pubblici

[ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore

[EFS.4] I punti di accesso EFS devono applicare un'identità utente

[EKS.1] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico

[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata

[EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata

[ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati

[ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito

[ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato

[ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati

[ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch

[ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa

[ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa

[ELB.3] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS

[ELB.4] Application Load Balancer deve essere configurato per eliminare le intestazioni http non valide

[ELB.8] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita che sia solida AWS Config Durata

[EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici

[EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata

[ES.2] I domini Elasticsearch non devono essere accessibili al pubblico

[ES.3] I domini Elasticsearch devono crittografare i dati inviati tra i nodi

[ES.5] I domini Elasticsearch devono avere la registrazione di controllo abilitata

[ES.8] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS

[EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata

[GuardDuty.1] GuardDuty dovrebbe essere abilitato

[GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata

[GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata

[GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato

[GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata

[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno

[IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console

[IAM.6] La MFA hardware deve essere abilitata per l'utente root

[IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide

[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse

[IAM.9] L'MFA deve essere abilitata per l'utente root

[IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola

[IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola

[IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero

[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password

[IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno

[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS

[IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM

[Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata

[Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata

[Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata

[Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata

[KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata

[Lambda.1] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico

[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati

[MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch

[MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker

[MSK.3] I connettori MSK Connect devono essere crittografati in transito

[Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch

[Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche

[Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software

[Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata

[RDS.13] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati

[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible

[RDS.20] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici delle istanze di database

[RDS.21] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database

[RDS.22] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database

[RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato

[RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato

[RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch

[] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato

[RDS.36] Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch

[RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch

[RDS.9] Le istanze DB RDS devono pubblicare i log in Logs CloudWatch

[Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico

[Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate

[Redshift.2] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito

[Redshift.4] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata

[Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS

[S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate

[S3.15] I bucket generici S3 devono avere Object Lock abilitato

[S3.17] I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys

[S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate

[S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto

[S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto

[S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate

[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS

[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico

[S3.9] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata

[SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet

[SecretsManager.1] I segreti di Secrets Manager devono avere la rotazione automatica abilitata

[SecretsManager.2] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente

[SecretsManager.4] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni

[SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch

[SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT

[StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata

[Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint

[WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata

[WAF.11] AWS WAF la registrazione ACL web deve essere abilitata

Profilo CRI v2.2 nel Security Hub CSPM

Il CRI Profile è un framework di sicurezza informatica sviluppato dal Cyber Risk Institute (CRI), una coalizione senza scopo di lucro di istituzioni finanziarie e associazioni di categoria. Il framework armonizza la sicurezza informatica e le aspettative normative per il settore dei servizi finanziari in una serie di requisiti comuni. Ciò consente a un'organizzazione di valutare se stessa una sola volta e di riferire in base a più normative. Per ulteriori informazioni sul framework e sui relativi requisiti, consulta la panoramica del profilo CRI sul sito Web del Cyber Risk Institute.

AWS Security Hub CSPM fornisce controlli di sicurezza che supportano un sottoinsieme di requisiti CRI Profile v2.2. I controlli eseguono controlli di sicurezza automatici per determinate risorse. Servizi

AWS Per abilitare e gestire questi controlli, è possibile abilitare CRI Profile v2.2 come standard in Security Hub CSPM. Tieni presente che i controlli non supportano i requisiti del profilo CRI v2.2 che richiedono controlli manuali.

L'attivazione di questo standard e il superamento dei relativi controlli non stabiliscono o certificano di per sé la conformità al CRI Profile v2.2. La conformità dipende dalle pratiche organizzative e operative che Security Hub CSPM non è in grado di valutare.

Argomenti

- Controlli che si applicano allo standard

Controlli che si applicano allo standard

L'elenco seguente specifica quali controlli CSPM di Security Hub si applicano al profilo CRI v2.2. Per esaminare i dettagli di un controllo, scegli il controllo.

- [Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato
- [ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- [Amplify.2] I rami Amplify devono essere etichettati
- [APIGateway.1] API Gateway REST e la registrazione dell'esecuzione dell' WebSocket API devono essere abilitati
- [APIGateway.2] Le fasi API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend
- [APIGateway.3] Le fasi API REST di API Gateway dovrebbero avere AWS X-Ray tracciamento abilitato
- [APIGateway.4] API Gateway deve essere associato a un ACL Web WAF
- [APIGateway.5] I dati della cache dell'API REST di API Gateway devono essere crittografati quando sono inattivi
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati

- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata
- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [Athena.4] I gruppi di lavoro Athena dovrebbero avere la registrazione abilitata
- [AutoScaling.1] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB
- [AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità
- [AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)
- [Autoscaling.5] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici
- [AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità
- [AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [Batch.2] Le politiche di pianificazione dei batch devono essere etichettate
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine

- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura
- [CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata
- [CloudTrail.3] Almeno un CloudTrail percorso deve essere abilitato
- [CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata
- [CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs
- [CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico
- [CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
- [CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»
- [CloudWatch.2] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate
- [CloudWatch.3] Assicurati che esistano un filtro metrico di registro e un allarme per l'accesso alla console di gestione senza MFA
- [CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM
- [CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrail alla configurazione
- [CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per Console di gestione AWS errori di autenticazione
- [CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione pianificata delle chiavi gestite dal cliente
- [CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3
- [CloudWatch.9] Assicurati che esistano un filtro metrico di registro e un allarme per AWS Config modifiche alla configurazione
- [CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza
- [CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)

- [CloudWatch.12] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gateway di rete
- [CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte
- [CloudWatch.14] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche al VPC
- [CloudWatch.15] gli CloudWatch allarmi dovrebbero avere azioni specificate configurate
- [CloudWatch.16] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato
- [CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate
- [CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili
- [CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato
- [CodeBuild.3] I log CodeBuild S3 devono essere crittografati
- [CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]
- [CodeBuild.7] le esportazioni dei gruppi di CodeBuild report devono essere crittografate quando sono inattive
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate
- [Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [DataSync.1] DataSync le attività dovrebbero avere la registrazione abilitata
- [DataSync.2] le DataSync attività devono essere etichettate
- [DMS.1] Le istanze di replica del Database Migration Service non devono essere pubbliche

- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.1] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda
- [DynamoDB.2] Le tabelle DynamoDB dovrebbero avere il ripristino point-in-time abilitato
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup
- [DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.1] Le istantanee di Amazon EBS non devono essere configurate per essere ripristinabili pubblicamente
- [EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita

- [EC2.3] I volumi Amazon EBS collegati devono essere crittografati quando sono inattivi
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC
- [EC2.7] La crittografia predefinita di EBS deve essere abilitata
- [EC2.8] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.9] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico
- [EC2.10] Amazon EC2 deve essere configurato per utilizzare gli endpoint VPC creati per il servizio Amazon EC2
- [EC2.12] Gli EIP Amazon EC2 non utilizzati devono essere rimossi
- [EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22
- [EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
- [EC2.15] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici
- [EC2.16] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse
- [EC2.17] Le istanze Amazon EC2 non devono utilizzare più ENI
- [EC2.18] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate
- [EC2.19] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio
- [EC2.20] Entrambi i tunnel VPN per un AWS Site-to-Site La connessione VPN dovrebbe essere attiva
- [EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata

- [EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto
- [EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.174] I set di opzioni DHCP EC2 devono essere etichettati
- [EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag
- [ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata
- [ECS.2] Ai servizi ECS non dovrebbero essere assegnati automaticamente indirizzi IP pubblici
- [ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host
- [ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati
- [ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root
- [ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore
- [ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione
- [ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate
- [ECS.12] I cluster ECS devono utilizzare Container Insights
- [ECS.16] I set di attività ECS non devono assegnare automaticamente indirizzi IP pubblici
- [ECS.17] Le definizioni delle attività ECS non devono utilizzare la modalità di rete host
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS

- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio
- [EFS.7] I file system EFS devono avere i backup automatici abilitati
- [EFS.8] I file system EFS devono essere crittografati quando sono inattivi
- [EKS.1] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico
- [EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata
- [EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [ELB.1] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [ELB.3] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS
- [ELB.4] Application Load Balancer deve essere configurato per eliminare le intestazioni http non valide
- [ELB.5] La registrazione di Application e Classic Load Balancers deve essere abilitata

- [ELB.6] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata
- [ELB.7] I Classic Load Balancer dovrebbero avere abilitato il drenaggio della connessione
- [ELB.8] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita che sia solida AWS Config Durata
- [ELB.9] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato
- [ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità
- [ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.16] Application Load Balancers deve essere associato a un AWS WAF ACL Web
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- [ELB.21] I gruppi target di Application e Network Load Balancer devono utilizzare protocolli di controllo dello stato crittografati
- [ELB.22] I gruppi target ELB devono utilizzare protocolli di trasporto crittografati
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo
- [EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito
- [ES.1] I domini Elasticsearch devono avere la crittografia a riposo abilitata
- [ES.2] I domini Elasticsearch non devono essere accessibili al pubblico
- [ES.3] I domini Elasticsearch devono crittografare i dati inviati tra i nodi
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [ES.5] I domini Elasticsearch devono avere la registrazione di controllo abilitata
- [ES.6] I domini Elasticsearch devono avere almeno tre nodi di dati

- [ES.7] I domini Elasticsearch devono essere configurati con almeno tre nodi master dedicati
- [ES.8] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS
- [EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ
- [FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione
- [Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.1] GuardDuty dovrebbe essere abilitato
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato
- [GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato
- [GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata
- [GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata
- [GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console

- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
- [IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
- [IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
- [IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
- [IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
- [IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
- [IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi

- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [KMS.3] AWS KMS keys non devono essere eliminati involontariamente
- [KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata
- [KMS.5] Le chiavi KMS non devono essere accessibili al pubblico
- [Lambda.1] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico
- [Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati
- [Lambda.3] Le funzioni Lambda devono trovarsi in un VPC
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker
- [MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata

- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata
- [RDS.1] L'istantanea RDS deve essere privata
- [RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible
- [RDS.3] Le istanze DB RDS devono avere la crittografia a riposo abilitata

- [RDS.4] Gli snapshot del cluster RDS e gli snapshot del database devono essere crittografati quando sono inattivi
- [RDS.5] Le istanze DB RDS devono essere configurate con più zone di disponibilità
- [RDS.6] Il monitoraggio avanzato deve essere configurato per le istanze DB RDS
- [RDS.7] I cluster RDS devono avere la protezione da eliminazione abilitata
- [RDS.8] Le istanze DB RDS devono avere la protezione da eliminazione abilitata
- [RDS.9] Le istanze DB RDS devono pubblicare i log in Logs CloudWatch
- [RDS.10] L'autenticazione IAM deve essere configurata per le istanze RDS
- [RDS.11] Le istanze RDS devono avere i backup automatici abilitati
- [RDS.12] L'autenticazione IAM deve essere configurata per i cluster RDS
- [RDS.13] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.15] I cluster RDS DB devono essere configurati per più zone di disponibilità
- [RDS.16] I cluster Aurora DB devono essere configurati per copiare i tag nelle istantanee DB
- [RDS.17] Le istanze DB RDS devono essere configurate per copiare i tag negli snapshot
- [RDS.19] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici del cluster
- [RDS.20] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici delle istanze di database
- [RDS.21] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database
- [RDS.22] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database
- [RDS.23] Le istanze RDS non devono utilizzare una porta predefinita del motore di database
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.26] Le istanze DB RDS devono essere protette da un piano di backup
- [RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch

- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.36] Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch
- [RDS.38] Le istanze DB RDS per PostgreSQL devono essere crittografate in transito
- [RDS.39] Le istanze DB RDS per MySQL devono essere crittografate in transito
- [RDS.41] Le istanze DB di RDS per SQL Server devono essere crittografate in transito
- [RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico
- [Redshift.2] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito
- [Redshift.3] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate
- [Redshift.4] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata
- [Redshift.6] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati
- [Redshift.7] I cluster Redshift devono utilizzare un routing VPC avanzato
- [Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate
- [Redshift.16] I gruppi di sottoreti del cluster Redshift devono avere sottoreti provenienti da più zone di disponibilità
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS

- [S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.2] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura
- [S3.3] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura
- [S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS
- [S3.6] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS
- [S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni
- [S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico
- [S3.9] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata
- [S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita
- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- [S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3
- [S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita
- S3.14[] I bucket S3 per uso generico devono avere il controllo delle versioni abilitato
- [S3.15] I bucket generici S3 devono avere Object Lock abilitato
- [S3.17] I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys
- [S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata
- [S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto
- [S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1

- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate
- [SecretsManager.1] I segreti di Secrets Manager devono avere la rotazione automatica abilitata
- [SecretsManager.2] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente
- [SecretsManager.3] Rimuovi i segreti inutilizzati di Secrets Manager
- [SecretsManager.4] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni
- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SNS.1] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS
- [SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.1] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager
- [SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch
- [SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT
- [SSM.4] I documenti SSM non devono essere pubblici
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata
- [Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [Transfer.6] I connettori Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola

- [WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WAF.11] AWS WAF la registrazione ACL web deve essere abilitata
- [WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Service-managed standard nel Security Hub CSPM

Uno standard gestito dai servizi è uno standard di sicurezza Servizio AWS gestito da un altro ma che è possibile visualizzare in Security Hub CSPM. Ad esempio, Service-Managed Standard: AWS Control Towerè uno standard gestito dai servizi che gestisce. AWS Control Tower Uno standard gestito dai servizi si differenzia da uno standard di sicurezza gestito da AWS Security Hub CSPM nei seguenti modi:

- Creazione ed eliminazione di standard: è possibile creare ed eliminare uno standard gestito dal servizio con la console o l'API del servizio di gestione oppure con. AWS CLI Finché non crei lo standard nel servizio di gestione in uno di questi modi, lo standard non viene visualizzato nella console CSPM di Security Hub e non è accessibile tramite l'API CSPM di Security Hub o. AWS CLI
- Nessuna attivazione automatica dei controlli: quando si crea uno standard gestito dal servizio, Security Hub CSPM e il servizio di gestione non abilitano automaticamente i controlli che si applicano allo standard. Inoltre, quando Security Hub CSPM rilascia nuovi controlli per lo standard, questi non vengono abilitati automaticamente. Si tratta di un allontanamento dagli standard gestiti da Security Hub CSPM. Per ulteriori informazioni sul modo consueto di configurare i controlli in Security Hub CSPM, vedere. Comprendere i controlli di sicurezza in Security Hub CSPM
- Abilitazione e disabilitazione dei controlli: consigliamo di abilitare e disabilitare i controlli nel servizio di gestione per evitare deviazioni.
- Disponibilità dei controlli: il servizio di gestione sceglie quali controlli sono disponibili come parte dello standard di gestione dei servizi. I controlli disponibili possono includere tutti o un sottoinsieme dei controlli CSPM esistenti di Security Hub.

Dopo che il servizio di gestione ha creato lo standard gestito dal servizio e reso disponibili i relativi controlli, puoi accedere ai risultati del controllo, agli stati dei controlli e al punteggio di sicurezza standard nella console CSPM di Security Hub, nell'API CSPM di Security Hub o. AWS CLI Alcune o tutte queste informazioni potrebbero essere disponibili anche nel servizio di gestione.

Seleziona uno standard gestito dal servizio dall'elenco seguente per visualizzare ulteriori dettagli al riguardo.

Service-managed standard

- Service-Managed Norma: AWS Control Tower

Service-Managed Norma: AWS Control Tower

Questa sezione fornisce informazioni su Service-Managed Standard:. AWS Control Tower

Che cos'è Service-Managed Standard: AWS Control Tower?

Service-Managed Standard: AWS Control Tower è uno standard gestito dai servizi che AWS Control Tower gestisce che supporta un sottoinsieme di controlli Security Hub. Questo standard è progettato per gli utenti di AWS Security Hub CSPM e. AWS Control Tower Consente di configurare i controlli di rilevamento di Security Hub CSPM dal AWS Control Tower servizio.

I controlli investigativi rilevano la non conformità delle risorse (ad esempio, configurazioni errate) all'interno dell'azienda. Account AWS

> **Tip**
>
> Service-managed gli standard differiscono dagli standard gestiti da AWS Security Hub CSPM. Ad esempio, è necessario creare ed eliminare uno standard gestito dal servizio di gestione. Per ulteriori informazioni, consulta Service-managed standard nel Security Hub CSPM.

Quando abiliti un controllo CSPM di Security Hub tramite AWS Control Tower, Control Tower abilita anche Security Hub CSPM per te in quegli account e regioni specifici, se non è già abilitato. Nella console CSPM e nell'API di Security Hub, puoi visualizzare Service-Managed Standard: AWS Control Tower insieme ad altri standard CSPM di Security Hub, una volta abilitato lo standard da. AWS Control Tower

Per ulteriori informazioni su questo standard, consulta i controlli CSPM di Security Hub nella Guida per l'AWS Control Tower utente.

Creazione dello standard

Questo standard è disponibile in Security Hub CSPM solo se si abilitano i controlli CSPM di Security Hub da. AWS Control Tower AWS Control Tower crea lo standard quando si abilita per la prima volta un controllo applicabile utilizzando uno dei seguenti metodi:

- AWS Control Tower console
- AWS Control Tower API (chiama l'`EnableControl`API)
- AWS CLI (esegui il `enable-control`comando)

Quando abiliti un controllo CSPM di Security Hub tramite AWS Control Tower, se non hai già abilitato Security Hub CSPM, abilita anche AWS Control Tower Security Hub CSPM per te in quegli account e regioni specifici.

Per identificare un controllo CSPM di Security Hub tramite l'ID di controllo in Control Catalog, puoi utilizzare il campo `Implementation.Identifier` in. AWS Control Tower Questo campo è mappato all'ID di controllo CSPM di Security Hub e può essere utilizzato per filtrare un ID di controllo specifico. Per recuperare i metadati di controllo per uno specifico controllo CSPM di Security Hub (ad esempio, "CodeBuild.1«) in AWS Control Tower, puoi utilizzare l'API: `ListControls`

```
aws controlcatalog list-controls --filter '{"Implementations":
{"Identifiers":["CodeBuild.1"],"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

Non puoi visualizzare o accedere a questo standard nella console CSPM di Security Hub, nell'API CSPM di Security Hub o AWS CLI senza prima configurare e abilitare i controlli CSPM di AWS Control Tower Security Hub AWS Control Tower utilizzando uno dei metodi precedenti.

Questo standard è disponibile solo dove è disponibile.Regioni AWSAWS Control Tower

Abilitazione e disabilitazione dei controlli nello standard

Dopo aver abilitato i controlli CSPM di Security Hub AWS Control Tower e aver creato lo AWS Control Tower standard Service-Managed Standard:, puoi visualizzare lo standard e i relativi controlli disponibili in Security Hub CSPM.

Quando Security Hub CSPM aggiunge nuovi controlli allo Service-Managed Standard: AWS Control Tower standard, questi non vengono abilitati automaticamente per i clienti che hanno lo standard

abilitato. È necessario abilitare e disabilitare i controlli per lo standard AWS Control Tower utilizzando uno dei seguenti metodi:

- AWS Control Tower console
- AWS Control Tower API (chiama le `DisableControl`API `EnableControl`and)
- AWS CLI (esegui i `disable-control`comandi `enable-control`and)

Quando si modifica lo stato di attivazione di un controllo in AWS Control Tower, la modifica si riflette anche in Security Hub CSPM.

Tuttavia, la disabilitazione di un controllo in Security Hub CSPM abilitato in AWS Control Tower comporta una deriva del controllo. Lo stato del controllo in viene visualizzato come. AWS Control Tower `Drifted` È possibile risolvere questa deriva utilizzando l'ResetEnabledControlAPI per reimpostare il controllo in corso, selezionando Re-register OU nella AWS Control Tower console o disabilitando e riabilitando il controllo AWS Control Tower utilizzando uno dei metodi precedenti.

Il completamento delle azioni di attivazione e disabilitazione in consente di evitare la deriva del controllo. AWS Control Tower

Quando abiliti o disabiliti i controlli in AWS Control Tower, l'azione si applica a tutti gli account e alle regioni governati da. AWS Control Tower Se abiliti e disabiliti i controlli in Security Hub CSPM (non consigliato per questo standard), l'azione si applica solo all'account e alla regione correnti.

> **Note**
>
> La configurazione centrale non può essere utilizzata per gestire Service-Managed Standard:. AWS Control Tower Puoi utilizzare solo il AWS Control Tower servizio per abilitare e disabilitare i controlli in questo standard.

Visualizzazione dello stato di attivazione e dello stato di controllo

È possibile visualizzare lo stato di attivazione di un controllo utilizzando uno dei seguenti metodi:

- Console CSPM Security Hub, API CSPM Security Hub o AWS CLI
- AWS Control Tower console
- AWS Control Tower API per visualizzare un elenco di controlli abilitati (chiama l'`ListEnabledControls`API)

- AWS CLI per visualizzare un elenco di controlli abilitati (esegui il `list-enabled-controls`comando)

Un controllo che disabiliti AWS Control Tower ha lo stato di attivazione in Security Hub CSPM, `Disabled` a meno che non abiliti esplicitamente tale controllo in Security Hub CSPM.

Security Hub CSPM calcola lo stato del controllo in base allo stato del flusso di lavoro e allo stato di conformità dei risultati del controllo. Per ulteriori informazioni sullo stato di attivazione e sullo stato di controllo, vedere. Revisione dei dettagli dei controlli in Security Hub CSPM

In base agli stati di controllo, Security Hub CSPM calcola un punteggio di sicurezza per Standard:. Service-Managed AWS Control Tower Questo punteggio è disponibile solo in Security Hub CSPM. Inoltre, è possibile visualizzare i risultati del controllo solo in Security Hub CSPM. Il punteggio di sicurezza standard e i risultati del controllo non sono disponibili in. AWS Control Tower

> **Note**
>
> Quando abiliti i controlli per Service-Managed Standard: AWS Control Tower, Security Hub CSPM può impiegare fino a 18 ore per generare risultati per i controlli che utilizzano una regola esistente collegata al AWS Config servizio. Potresti avere regole collegate ai servizi esistenti se hai abilitato altri standard e controlli in Security Hub CSPM. Per ulteriori informazioni, consulta Pianificazione dell'esecuzione dei controlli di sicurezza.

Eliminazione dello standard

È possibile eliminare questo standard gestito AWS Control Tower dal servizio disabilitando tutti i controlli applicabili utilizzando uno dei seguenti metodi:

- AWS Control Tower console
- AWS Control Tower API (chiama l'`DisableControl`API)
- AWS CLI (esegui il `disable-control`comando)

La disabilitazione di tutti i controlli elimina lo standard in tutti gli account gestiti e nelle regioni governate in. AWS Control Tower L'eliminazione dello standard lo AWS Control Tower rimuove dalla pagina Standard della console CSPM di Security Hub e non è più possibile accedervi utilizzando l'API CSPM di Security Hub o. AWS CLI

> **Note**
>
> La disabilitazione di tutti i controlli dallo standard in Security Hub CSPM non disabilita o elimina lo standard.

La disattivazione del servizio CSPM di Security Hub rimuove Service-Managed Standard AWS Control Tower e tutti gli altri standard che hai abilitato.

Ricerca del formato di campo per Standard: Service-Managed AWS Control Tower

Quando crei Service-Managed Standard: AWS Control Tower e ne abiliti i controlli, inizierai a ricevere i risultati del controllo in Security Hub CSPM. Security Hub CSPM riporta i risultati del controllo in. AWS Formato ASFF (Security Finding Format) Questi sono i valori ASFF per Amazon Resource Name (ARN) di questo standard e: `GeneratorId`

- ARN standard — *`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`*

Per un esempio di risultato per Service-Managed Standard: AWS Control Tower, vedereEsempi di risultati di controllo.

Controlli che si applicano a Service-Managed Standard: AWS Control Tower

Service-Managed Standard: AWS Control Tower supporta un sottoinsieme di controlli che fanno parte dello standard AWS Foundational Security Best Practices (FSBP). Scegliete un controllo per visualizzarne le informazioni, incluse le procedure di correzione in caso di risultati non riusciti.

Per vedere da cosa sono supportati i controlli CSPM di Security Hub AWS Control Tower, puoi utilizzare uno dei seguenti metodi:

- AWS Controlla la console Catalog per cui puoi filtrare "`Control owner = AWS Security Hub`"
- AWS L'API Control Catalog (chiama l'`ListControls`API) con filtro `Implementations` per cui verificare `Types` è `AWS::SecurityHub::SecurityControl`
- AWS CLI (esegui il `list-controls`comando) con filtro per`Implementations`. Esempio di comando CLI:

```
aws controlcatalog list-controls --filter '{"Implementations":{"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

I limiti regionali sui controlli CSPM di Security Hub, se abilitati tramite lo standard Control Tower, potrebbero non corrispondere ai limiti regionali sui controlli sottostanti.

In Security Hub CSPM, se i risultati del controllo consolidato sono disattivati nel tuo account, il `ProductFields.ControlId` campo dei risultati generati utilizza l'ID di controllo standard. L'ID di controllo basato su standard è formattato come CT. ***`ControlId`***(ad esempio,). CT.CodeBuild.1

Per ulteriori informazioni su questo standard, consulta i controlli CSPM di Security Hub nella Guida per l'AWS Control Tower utente.

Abilitazione di uno standard di sicurezza

Quando si abilita uno standard di sicurezza in AWS Security Hub CSPM, Security Hub CSPM crea e abilita automaticamente tutti i controlli che si applicano allo standard. Security Hub CSPM inizia anche a eseguire controlli di sicurezza e a generare risultati per i controlli.

Per ottimizzare la copertura e l'accuratezza dei risultati, abilita e configura la registrazione delle risorse AWS Config prima di abilitare uno standard. Quando configurate la registrazione delle risorse, assicuratevi anche di abilitarla per tutti i tipi di risorse controllate dai controlli che si applicano allo standard. In caso contrario, Security Hub CSPM potrebbe non essere in grado di valutare le risorse appropriate e generare risultati accurati per i controlli che si applicano allo standard. Per ulteriori informazioni, consulta Attivazione e configurazione AWS Config per Security Hub CSPM.

Gli standard di sicurezza multicloud, come CIS Azure Foundations Benchmark v4.0.0, hanno requisiti diversi dagli standard. AWS Gli standard multicloud richiedono un connettore CSPM Security Hub per il provider cloud esterno e non richiedono la configurazione AWS Config o la creazione manuale di un registratore di configurazione. Il connettore multicloud Security Hub CSPM configura automaticamente un registratore collegato al servizio per valutare le risorse nell'ambiente cloud esterno.

Dopo aver abilitato uno standard, è possibile disattivare o riattivare successivamente i singoli controlli che si applicano allo standard. Se si disabilita un controllo per uno standard, Security Hub CSPM interrompe la generazione dei risultati per il controllo. Inoltre, Security Hub CSPM ignora il controllo quando calcola il punteggio di sicurezza per lo standard. Il punteggio di sicurezza è la percentuale di

controlli che hanno superato la valutazione, rispetto al numero totale di controlli che si applicano allo standard, sono abilitati e dispongono di dati di valutazione.

Quando abiliti uno standard, Security Hub CSPM genera un punteggio di sicurezza preliminare per lo standard, in genere entro 30 minuti dalla prima visita alla pagina Riepilogo o Standard di sicurezza sulla console CSPM di Security Hub. I punteggi di sicurezza vengono generati solo per gli standard abilitati quando si visitano quelle pagine sulla console. Inoltre, la registrazione delle risorse deve essere configurata in AWS Config per visualizzare i punteggi. Nelle regioni della Cina e AWS GovCloud (US) Regions, possono essere necessarie fino a 24 ore prima che Security Hub CSPM generi un punteggio di sicurezza preliminare per uno standard. Dopo che Security Hub CSPM ha generato un punteggio preliminare, lo aggiorna ogni 24 ore. Per determinare quando un punteggio di sicurezza è stato aggiornato l'ultima volta, puoi fare riferimento a un timestamp fornito da Security Hub CSPM per il punteggio. Per ulteriori informazioni, consulta Calcolo dei punteggi di sicurezza.

Il modo in cui si abilita uno standard dipende dal fatto che si utilizzi la configurazione centrale per gestire Security Hub CSPM per più account e. Regioni AWS Si consiglia di utilizzare la configurazione centrale se si desidera abilitare gli standard in ambienti con più account e più regioni. È possibile utilizzare la configurazione centrale se si integra Security Hub CSPM con. AWS Organizations Se non si utilizza la configurazione centrale, è necessario abilitare ogni standard separatamente in ogni account e in ogni regione.

Argomenti

- Abilitazione di uno standard in più account e Regioni AWS
- Abilitare uno standard in un singolo account e Regione AWS
- Verifica dello stato di uno standard

Abilitazione di uno standard in più account e Regioni AWS

Per abilitare e configurare uno standard di sicurezza su più account e Regioni AWS utilizzare la configurazione centrale. Con la configurazione centrale, l'amministratore delegato di Security Hub CSPM può creare politiche di configurazione CSPM di Security Hub che abilitano uno o più standard. L'amministratore può quindi associare una politica di configurazione a singoli account, unità organizzative (OU) o root. Una politica di configurazione influisce sulla regione di origine, nota anche come regione di aggregazione, e su tutte le regioni collegate.

I criteri di configurazione offrono opzioni di personalizzazione. Ad esempio, è possibile scegliere di abilitare solo lo standard AWS Foundational Security Best Practices (FSBP) per un'unità organizzativa. Per un'altra unità organizzativa, puoi scegliere di abilitare sia lo standard FSBP

che lo standard Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0. Per informazioni sulla creazione di una politica di configurazione che abiliti gli standard particolari specificati dall'utente, vedere. Creazione e associazione di policy di configurazione

Se utilizzi la configurazione centrale, Security Hub CSPM non abilita automaticamente alcuno standard negli account nuovi o esistenti. Invece, l'amministratore CSPM di Security Hub specifica quali standard abilitare nei diversi account quando crea le politiche di configurazione CSPM di Security Hub per la propria organizzazione. Security Hub CSPM offre una politica di configurazione consigliata in cui è abilitato solo lo standard FSBP. Per ulteriori informazioni, consulta Tipi di politiche di configurazione.

> **Note**
>
> L'amministratore CSPM di Security Hub può utilizzare le politiche di configurazione per abilitare qualsiasi standard tranne lo standard gestito dai AWS Control Tower servizi. Per abilitare questo standard, l'amministratore deve utilizzare direttamente. AWS Control Tower Devono AWS Control Tower inoltre abilitare o disabilitare i singoli controlli di questo standard per un account gestito centralmente.

Se desideri che alcuni account abilitino e configurino gli standard per i propri account, l'amministratore CSPM di Security Hub può designare tali account come account autogestiti. Self-managed gli account devono abilitare e configurare gli standard separatamente in ciascuna regione.

Abilitare uno standard in un singolo account e Regione AWS

Se non utilizzi la configurazione centrale o disponi di un account autogestito, non puoi utilizzare le policy di configurazione per abilitare centralmente gli standard di sicurezza in più account o Regioni AWS. Tuttavia, puoi abilitare uno standard in un unico account e regione. È possibile farlo utilizzando la console CSPM di Security Hub o l'API CSPM di Security Hub.

Security Hub CSPM console

Segui questi passaggi per abilitare uno standard in un account e in una regione utilizzando la console Security Hub CSPM.

Per abilitare uno standard in un account e in un'unica regione

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri abilitare lo standard.
3. Nel riquadro di navigazione, scegli Standard di sicurezza. La pagina degli standard di sicurezza elenca tutti gli standard attualmente supportati da Security Hub CSPM. Se hai già abilitato uno standard, la sezione relativa allo standard include il punteggio di sicurezza corrente e dettagli aggiuntivi per lo standard.
4. Nella sezione relativa allo standard che desideri abilitare, scegli Abilita standard.

Per abilitare lo standard in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

Security Hub CSPM API

Per abilitare uno standard a livello di codice in un singolo account e regione, usa l'operazione. BatchEnableStandards Oppure, se stai usando il AWS Command Line Interface (AWS CLI), esegui il batch-enable-standardscomando.

Nella tua richiesta, utilizza il `StandardsArn` parametro per specificare l'Amazon Resource Name (ARN) dello standard che desideri abilitare. Specificate anche la regione a cui si riferisce la richiesta. Ad esempio, il comando seguente abilita lo standard AWS Foundational Security Best Practices (FSBP):

```
$ 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
```

*arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0*Dov'è l'ARN dello standard FSBP nella regione Stati Uniti orientali (Virginia settentrionale) ed *us-east-1* è la regione in cui abilitarlo.

Per ottenere l'ARN per uno standard, usa l'DescribeStandardsoperazione o, se stai usando il AWS CLI, esegui il comando. describe-standards

Per esaminare innanzitutto un elenco di standard attualmente abilitati nel tuo account, puoi utilizzare l'GetEnabledStandardsoperazione. Se utilizzi AWS CLI, puoi eseguire il comando get-enabled-standards per recuperare questo elenco.

Dopo aver abilitato uno standard, Security Hub CSPM inizia a eseguire attività per abilitare lo standard nell'account e nella regione specificata. Ciò include la creazione di tutti i controlli che si

applicano allo standard. Per monitorare lo stato di queste attività, puoi controllare lo stato dello standard per l'account e la regione.

Verifica dello stato di uno standard

Quando abiliti uno standard di sicurezza per un account, Security Hub CSPM inizia a creare tutti i controlli che si applicano allo standard nell'account. Security Hub CSPM esegue anche attività aggiuntive per abilitare lo standard per l'account, come la generazione di un punteggio di sicurezza preliminare per lo standard. Sebbene Security Hub CSPM esegua queste attività, lo stato dello standard è Pendingrelativo all'account. Lo stato dello standard passa quindi attraverso stati aggiuntivi, che è possibile monitorare e controllare.

> **Note**
>
> Le modifiche ai singoli controlli di uno standard non influiscono sullo stato generale dello standard. Ad esempio, se abiliti un controllo precedentemente disabilitato, la modifica non influisce sullo stato dello standard. Allo stesso modo, se modifichi il valore di un parametro per un controllo abilitato, la modifica non influisce sullo stato dello standard.

Per verificare lo stato di uno standard utilizzando la console CSPM di Security Hub, scegli Standard di sicurezza nel riquadro di navigazione. La pagina degli standard di sicurezza elenca tutti gli standard attualmente supportati da Security Hub CSPM. Se Security Hub CSPM sta attualmente eseguendo attività per abilitare lo standard, la sezione relativa allo standard indica che Security Hub CSPM sta ancora generando un punteggio di sicurezza per lo standard. Se uno standard è abilitato, la sezione relativa allo standard include il punteggio corrente. Scegli Visualizza risultati per esaminare ulteriori dettagli, incluso lo stato dei singoli controlli che si applicano allo standard. Per ulteriori informazioni, consulta Pianificazione dell'esecuzione dei controlli di sicurezza.

Per verificare lo stato di uno standard a livello di codice con l'API CSPM Security Hub, utilizzare l'operazione. GetEnabledStandards Nella tua richiesta, utilizza facoltativamente il `StandardsSubscriptionArns` parametro per specificare l'Amazon Resource Name (ARN) dello standard di cui desideri controllare lo stato. Se stai usando il AWS Command Line Interface (AWS CLI), puoi eseguire il comando get-enabled-standards per verificare lo stato di uno standard. Per specificare l'ARN dello standard da controllare, utilizzare il `standards-subscription-arns` parametro. Per determinare l'ARN da specificare, è possibile utilizzare l'DescribeStandardsoperazione o, per la AWS CLI, eseguire il describe-standardscomando.

Se la richiesta ha esito positivo, Security Hub CSPM risponde con una serie di oggetti. `StandardsSubscription` Un abbonamento standard è una AWS risorsa che Security Hub CSPM crea in un account quando uno standard è abilitato per l'account. Ogni `StandardsSubscription` oggetto fornisce dettagli su uno standard attualmente abilitato o in fase di attivazione o disabilitazione per l'account. All'interno di ogni oggetto, il `StandardsStatus` campo specifica lo stato corrente dello standard per l'account.

Lo stato di uno standard (`StandardsStatus`) può essere uno dei seguenti.

PENDING

Security Hub CSPM sta attualmente eseguendo attività per abilitare lo standard per l'account. Ciò include la creazione dei controlli che si applicano allo standard e la generazione di un punteggio di sicurezza preliminare per lo standard. Security Hub CSPM può impiegare diversi minuti per completare tutte le attività. Uno standard può avere questo stato anche se è già abilitato per l'account e Security Hub CSPM sta attualmente aggiungendo nuovi controlli allo standard.

Se uno standard ha questo stato, potresti non essere in grado di recuperare i dettagli dei singoli controlli che si applicano allo standard. Inoltre, potresti non essere in grado di configurare o disabilitare i singoli controlli per lo standard. Ad esempio, se si tenta di disabilitare un controllo utilizzando l'UpdateStandardsControloperazione, si verifica un errore.

Per determinare se è possibile configurare o gestire in altro modo i singoli controlli per lo standard, fate riferimento al valore del `StandardsControlsUpdatable` campo. Se il valore di questo campo è`READY_FOR_UPDATES`, puoi iniziare a gestire i singoli controlli per lo standard. Altrimenti, attendi che Security Hub CSPM completi le attività di elaborazione aggiuntive per abilitare lo standard.

READY

Lo standard è attualmente abilitato per l'account. Security Hub CSPM può eseguire controlli di sicurezza e generare risultati per tutti i controlli che si applicano allo standard e sono attualmente abilitati. Security Hub CSPM può anche calcolare un punteggio di sicurezza per lo standard.

Se uno standard ha questo stato, è possibile recuperare i dettagli dei singoli controlli che si applicano allo standard. Inoltre, puoi configurare, disabilitare o riattivare i controlli. Puoi anche disabilitare lo standard.

INCOMPLETE

Security Hub CSPM non è stato in grado di abilitare completamente lo standard per l'account. Security Hub CSPM non può eseguire controlli di sicurezza e generare risultati per tutti i controlli

che si applicano allo standard e sono attualmente abilitati. Inoltre, Security Hub CSPM non è in grado di calcolare un punteggio di sicurezza per lo standard.

Per gli standard multicloud, l'abbonamento viene sottoscritto `INCOMPLETE` con un motivo di status: `NO_AVAILABLE_MULTICLOUD_CONNECTOR` se si abilita lo standard senza un connettore CSPM. L'abbonamento passa automaticamente al momento in `READY` cui un connettore diventa disponibile.

Per determinare il motivo per cui lo standard non è stato possibile abilitare completamente, fate riferimento alle informazioni nell'`StandardsStatusReason`array. Questo array specifica i problemi che hanno impedito a Security Hub CSPM di abilitare lo standard. Se si è verificato un errore interno, prova ad abilitare nuovamente lo standard per l'account. Per altri tipi di problemi, controlla AWS Config le tue impostazioni. Puoi anche disabilitare i singoli controlli che non desideri controllare o disabilitare completamente lo standard.

DELETING

Security Hub CSPM sta attualmente elaborando una richiesta per disabilitare lo standard per l'account. Ciò include la disabilitazione dei controlli che si applicano allo standard e la rimozione del punteggio di sicurezza associato. Il completamento dell'elaborazione della richiesta da parte di Security Hub CSPM può richiedere alcuni minuti.

Se uno standard ha questo stato, non puoi riattivarlo o provare a disabilitarlo nuovamente per l'account. Security Hub CSPM deve prima completare l'elaborazione della richiesta corrente. Inoltre, non è possibile recuperare i dettagli dei singoli controlli che si applicano allo standard o gestire i controlli.

FAILED

Security Hub CSPM non è riuscito a disabilitare lo standard per l'account. Si sono verificati uno o più errori quando Security Hub CSPM ha tentato di disabilitare lo standard. Inoltre, Security Hub CSPM non è in grado di calcolare un punteggio di sicurezza per lo standard.

Per determinare il motivo per cui lo standard non è stato completamente disabilitato, fai riferimento alle informazioni nell'`StandardsStatusReason`array. Questo array specifica i problemi che hanno impedito a Security Hub CSPM di disabilitare lo standard.

Se uno standard ha questo stato, non è possibile recuperare i dettagli dei singoli controlli che si applicano allo standard o gestire i controlli. Tuttavia, puoi riattivare lo standard per l'account. Se risolvi i problemi che hanno impedito a Security Hub CSPM di disabilitare lo standard, puoi anche provare a disabilitare nuovamente lo standard.

Se lo stato di uno standard è`READY`, Security Hub CSPM esegue controlli di sicurezza e genera risultati per tutti i controlli che si applicano allo standard e che sono attualmente abilitati. Per altri stati, Security Hub CSPM potrebbe eseguire controlli e generare risultati per alcuni, ma non tutti, i controlli abilitati. La generazione o l'aggiornamento dei risultati dei controlli possono richiedere fino a 24 ore. Per ulteriori informazioni, consulta Pianificazione dell'esecuzione dei controlli di sicurezza.

Revisione dei dettagli di uno standard di sicurezza

Dopo aver abilitato uno standard di sicurezza in AWS Security Hub CSPM, puoi utilizzare la console per esaminare i dettagli dello standard. Sulla console, la pagina dei dettagli di uno standard include le seguenti informazioni:

- Il punteggio di sicurezza attuale dello standard.
- Una tabella di controlli che si applicano allo standard.
- Statistiche aggregate per i controlli che si applicano allo standard.
- Un riepilogo visivo dello stato dei controlli che si applicano allo standard.
- Un riepilogo visivo dei controlli di sicurezza per i controlli abilitati e applicabili allo standard. Se si esegue l'integrazione con AWS Organizations, i controlli abilitati in almeno un account dell'organizzazione vengono considerati abilitati.

Per esaminare questi dettagli, scegli Standard di sicurezza nel riquadro di navigazione sulla console. Quindi, nella sezione relativa allo standard, scegli Visualizza risultati. Per un'analisi più approfondita, puoi filtrare e ordinare i dati e approfondire i dettagli dei singoli controlli che si applicano allo standard.

Argomenti

- Comprensione del punteggio di sicurezza standard
- Revisione dei controlli per uno standard

Comprensione del punteggio di sicurezza standard

Nella console AWS Security Hub CSPM, la pagina dei dettagli di uno standard mostra il punteggio di sicurezza per lo standard. Il punteggio è la percentuale di controlli che hanno superato la valutazione, rispetto al numero totale di controlli che si applicano allo standard, sono abilitati e dispongono di dati di valutazione. Sotto il punteggio c'è un grafico che riassume i controlli di sicurezza per i controlli abilitati per lo standard. Ciò include il numero di controlli di sicurezza superati e non riusciti. Per gli account amministratore, il punteggio e il grafico standard vengono aggregati per l'account

amministratore e per tutti gli account dei membri. Per esaminare i controlli di sicurezza non riusciti relativi ai controlli con una gravità specifica, scegli la gravità.

Quando abiliti uno standard, Security Hub CSPM genera un punteggio di sicurezza preliminare per lo standard, in genere entro 30 minuti dalla prima visita alla pagina Riepilogo o alla pagina degli standard di sicurezza sulla console CSPM di Security Hub. I punteggi vengono generati solo per gli standard abilitati quando si visitano quelle pagine. Inoltre, la registrazione AWS Config delle risorse deve essere configurata per visualizzare gli spartiti. Nelle regioni della Cina e AWS GovCloud (US) Regions, possono essere necessarie fino a 24 ore prima che Security Hub CSPM generi un punteggio preliminare. Dopo che Security Hub CSPM ha generato un punteggio preliminare per uno standard, lo aggiorna ogni 24 ore. Per ulteriori informazioni, consulta Calcolo dei punteggi di sicurezza.

Tutti i dati nelle pagine dei dettagli degli standard di sicurezza sono specifici di quelli correnti, a Regione AWS meno che non si imposti una regione di aggregazione. Se imposti una regione di aggregazione, i punteggi di sicurezza si applicano a tutte le regioni e includono i risultati per tutte le aree collegate. Inoltre, lo stato di conformità dei controlli riflette i risultati delle regioni collegate e il numero di controlli di sicurezza include i risultati delle regioni collegate.

Revisione dei controlli per uno standard

Quando si utilizza la console AWS Security Hub CSPM per esaminare i dettagli di uno standard abilitato, è possibile esaminare una tabella dei controlli di sicurezza applicabili allo standard. Per ogni controllo, la tabella include le seguenti informazioni:

- L'ID e il titolo del controllo.
- Lo stato del controllo. Per ulteriori informazioni, consulta Valutazione dello stato di conformità e dello stato di controllo.
- La severità assegnata al controllo.
- Il numero di controlli non riusciti e il numero totale di controlli. Se applicabile, il campo Controlli falliti specifica anche il numero di risultati con lo stato Sconosciuto.
- Se il controllo supporta parametri personalizzati. Per ulteriori informazioni, consulta Comprensione dei parametri di controllo in Security Hub CSPM.

Security Hub CSPM aggiorna gli stati di controllo e il conteggio dei controlli di sicurezza ogni 24 ore. Un timestamp nella parte superiore della pagina indica quando Security Hub CSPM ha aggiornato questi dati per l'ultima volta.

Per gli account amministratore, gli stati di controllo e il numero di controlli di sicurezza sono aggregati tra l'account amministratore e tutti gli account dei membri. Il numero di controlli abilitati include i controlli abilitati per lo standard nell'account amministratore o in almeno un account membro. Il numero di controlli disabilitati include i controlli disabilitati per lo standard nell'account amministratore e in tutti gli account dei membri.

È possibile filtrare la tabella dei controlli che si applicano allo standard. Utilizzando le opzioni Filtra per accanto alla tabella, è possibile scegliere di visualizzare solo i controlli abilitati o disabilitati per lo standard. Se si visualizzano solo i controlli abilitati, è possibile filtrare ulteriormente la tabella in base allo stato del controllo. È quindi possibile concentrarsi sui controlli con uno stato di controllo specifico. Oltre alle opzioni Filtra per, puoi inserire criteri di filtro nella casella Filtra controlli. Ad esempio, è possibile filtrare per ID o titolo del controllo.

Scegli il tuo metodo di accesso preferito. Quindi segui i passaggi per rivedere i controlli che si applicano a uno standard che hai abilitato.

Security Hub CSPM console

Per esaminare i controlli di uno standard abilitato

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Scegli Standard di sicurezza nel pannello di navigazione.
3. Nella sezione relativa allo standard, scegli Visualizza risultati.

La tabella in fondo alla pagina elenca tutti i controlli che si applicano allo standard. È possibile filtrare e ordinare la tabella. Puoi anche scaricare la pagina corrente della tabella come file CSV. Per fare ciò, scegli Scarica sopra la tabella. Se filtri la tabella, il file scaricato include solo i controlli che corrispondono alle impostazioni correnti del filtro.

Security Hub CSPM API

Per esaminare i controlli per uno standard abilitato

1. Utilizza il ListSecurityControlDefinitionsfunzionamento dell'API CSPM Security Hub. Se stai usando AWS CLI, esegui il comando list-security-control-definitions.

   Specificate l'Amazon Resource Name (ARN) dello standard per cui desiderate esaminare i controlli. Per ottenere ARN per gli standard, usa l'DescribeStandardsoperazione o esegui

il comando describe-standards. Se non si specifica l'ARN per uno standard, Security Hub CSPM restituisce tutti gli ID di controllo di sicurezza.

2. Utilizza il ListStandardsControlAssociationsfunzionamento dell'API CSPM Security Hub o esegui il comando list-standards-control-associations. Questa operazione indica in quali standard è abilitato un controllo.

   Identifica il controllo fornendo l'ID o l'ARN del controllo di sicurezza. I parametri di impaginazione sono opzionali.

L'esempio seguente indica in quali standard è abilitato il Config.1 controllo.

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

Disattivazione degli standard di sicurezza abilitati automaticamente

Se l'organizzazione non utilizza la configurazione centrale, utilizza un tipo di configurazione chiamato configurazione locale. Con la configurazione locale, AWS Security Hub CSPM può abilitare automaticamente gli standard di sicurezza predefiniti per gli account dei nuovi membri quando gli account entrano a far parte dell'organizzazione. Tutti i controlli che si applicano a questi standard predefiniti vengono inoltre abilitati automaticamente.

Attualmente, gli standard di sicurezza predefiniti sono lo standard AWS Foundational Security Best Practices e lo standard Center for Internet Security (CIS AWS) Foundations Benchmark v1.2.0. Per informazioni su questi standard, consulta la. Riferimento agli standard per Security Hub CSPM

Se preferisci abilitare manualmente gli standard di sicurezza per gli account dei nuovi membri, puoi disattivare l'abilitazione automatica degli standard predefiniti. È possibile farlo solo se si integra AWS Organizations e si utilizza la configurazione locale. Se si utilizza la configurazione centrale, è possibile invece creare una politica di configurazione che abiliti gli standard predefiniti e associare la politica alla radice. Tutti gli account e le unità organizzative dell'organizzazione ereditano quindi questa politica di configurazione a meno che non siano associati a una politica diversa o siano gestiti automaticamente. Se non esegui l'integrazione con AWS Organizations, puoi disabilitare uno standard predefinito quando attivi inizialmente Security Hub CSPM o versioni successive. Per scoprire come, consulta Disabilitazione di uno standard.

Per disattivare l'abilitazione automatica degli standard predefiniti per i nuovi account membro, puoi utilizzare la console CSPM di Security Hub o l'API CSPM di Security Hub.

Security Hub CSPM console

Segui questi passaggi per disattivare l'abilitazione automatica degli standard predefiniti utilizzando la console Security Hub CSPM.

Per disattivare l'attivazione automatica degli standard predefiniti

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore.
2. Nel riquadro di navigazione, in Impostazioni, scegli Configurazione.
3. Nella sezione Panoramica, scegli Modifica.
4. In Nuove impostazioni dell'account, deseleziona la casella di controllo Abilita gli standard di sicurezza predefiniti.
5. Scegli Conferma.

Security Hub CSPM API

Per disattivare l'abilitazione automatica degli standard predefiniti a livello di codice, dall'account amministratore CSPM di Security Hub, utilizzare il funzionamento dell'API CSPM di UpdateOrganizationConfigurationSecurity Hub. Nella richiesta, specificare il parametro. `NONE` `AutoEnableStandards`

Se utilizzi il AWS CLI, esegui il update-organization-configurationcomando per disattivare l'abilitazione automatica degli standard predefiniti. Per il parametro `auto-enable-standards`, specifica `NONE`. Ad esempio, il comando seguente abilita automaticamente Security Hub CSPM per gli account dei nuovi membri e disattiva l'abilitazione automatica degli standard predefiniti per gli account.

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-standards NONE
```

Disabilitazione di uno standard di sicurezza

Quando si disabilita uno standard di sicurezza in AWS Security Hub CSPM, si verifica quanto segue:

- Tutti i controlli che si applicano allo standard sono disabilitati, a meno che non siano associati a un altro standard attualmente abilitato.
- I controlli di sicurezza per i controlli disattivati non vengono più eseguiti e non vengono generati risultati aggiuntivi per i controlli disattivati.
- I risultati esistenti relativi ai controlli disattivati vengono archiviati automaticamente dopo circa 3-5 giorni.
- AWS Config le regole che Security Hub CSPM ha creato per i controlli disabilitati vengono eliminate.

L'eliminazione delle AWS Config regole appropriate avviene in genere entro pochi minuti dalla disattivazione di uno standard. Tuttavia, l'operazione potrebbe richiedere più tempo. Se la prima richiesta non riesce a eliminare le regole, Security Hub CSPM riprova ogni 12 ore. Tuttavia, se hai disabilitato Security Hub CSPM o non hai abilitato nessun altro standard, Security Hub CSPM non può riprovare, il che significa che non può eliminare le regole. Se ciò si verifica e devi eliminare le regole, contatta. Supporto AWS

> **Note**
>
> La disabilitazione di uno standard può aumentare AWS Config i costi legati alla disabilitazione delle regole associate. Prima di disabilitare qualsiasi standard, ti consigliamo di consultare la documentazione relativa alle considerazioni sull'eliminazione AWS Config delle regole. Scopri anche come escludere gli elementi di configurazione Resource Compliance dalla registrazione quando le regole legate a uno standard CSPM di Security Hub sono disabilitate.

Argomenti

- Disabilitazione di uno standard in più account e Regioni AWS
- Disabilitazione di uno standard in un singolo account e Regione AWS

Disabilitazione di uno standard in più account e Regioni AWS

Per disabilitare uno standard di sicurezza su più account e utilizzare Regioni AWS la configurazione centrale. Con la configurazione centrale, l'amministratore delegato di Security Hub CSPM può creare politiche di configurazione CSPM di Security Hub che disabilitano uno o più standard. L'amministratore può quindi associare una politica di configurazione a singoli account, unità organizzative (OU) o root. Una politica di configurazione influisce sulla regione di origine, nota anche come regione di aggregazione, e su tutte le regioni collegate.

I criteri di configurazione offrono opzioni di personalizzazione. Ad esempio, è possibile scegliere di disabilitare il Payment Card Industry Data Security Standard (PCI DSS) in un'unica unità organizzativa. Per un'altra unità organizzativa, è possibile scegliere di disabilitare sia lo standard PCI DSS che lo standard SP 800-53 Rev. 5 del National Institute of Standards and Technology (NIST). Per informazioni sulla creazione di una politica di configurazione che abiliti o disabiliti i singoli standard specificati, vedere. Creazione e associazione di policy di configurazione

> **Note**
>
> L'amministratore CSPM di Security Hub può utilizzare le politiche di configurazione per disabilitare qualsiasi standard tranne lo standard gestito dai AWS Control Tower servizi. Per disabilitare questo standard, l'amministratore deve utilizzare direttamente. AWS Control Tower Devono inoltre AWS Control Tower disabilitare o abilitare i controlli individuali di questo standard per un account gestito centralmente.

Se desideri che alcuni account configurino o disabilitino gli standard per i propri account, l'amministratore CSPM di Security Hub può designare tali account come account autogestiti. Self-managed gli account devono disabilitare gli standard separatamente in ciascuna regione.

Disabilitazione di uno standard in un singolo account e Regione AWS

Se non utilizzi la configurazione centrale o disponi di un account autogestito, non puoi utilizzare i criteri di configurazione per disabilitare centralmente gli standard di sicurezza in più account o. Regioni AWS Tuttavia, puoi disabilitare uno standard in un unico account e regione. È possibile farlo utilizzando la console CSPM di Security Hub o l'API CSPM di Security Hub.

Security Hub CSPM console

Segui questi passaggi per disabilitare uno standard in un account e in una regione utilizzando la console Security Hub CSPM.

Per disabilitare uno standard in un account e in una regione

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri disabilitare lo standard.
3. Nel riquadro di navigazione, scegli Standard di sicurezza.
4. Nella sezione relativa allo standard che desideri disabilitare, scegli Disabilita standard.

Per disabilitare lo standard in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

Security Hub CSPM API

Per disabilitare uno standard a livello di codice in un singolo account e regione, usa l'operazione. BatchDisableStandards Oppure, se stai usando il AWS Command Line Interface (AWS CLI), esegui il batch-disable-standardscomando.

Nella tua richiesta, utilizza il `StandardsSubscriptionArns` parametro per specificare l'Amazon Resource Name (ARN) dello standard che desideri disabilitare. Se si utilizza il AWS CLI, utilizzare il `standards-subscription-arns` parametro per specificare l'ARN. Specificate anche la regione a cui si riferisce la richiesta. Ad esempio, il comando seguente disabilita lo standard AWS Foundational Security Best Practices (FSBP) per un account (): *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
```

*arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0*Dov'è l'ARN dello standard FSBP per l'account nella regione Stati Uniti orientali (Virginia settentrionale) ed *us-east-1* è la regione in cui disabilitarlo.

Per ottenere l'ARN per uno standard, è possibile utilizzare l'GetEnabledStandardsoperazione. Questa operazione recupera informazioni sugli standard attualmente abilitati nel tuo account.

Se utilizzi il AWS CLI, puoi eseguire il comando get-enabled-standards per recuperare queste informazioni.

Dopo aver disabilitato uno standard, Security Hub CSPM inizia a eseguire attività per disabilitare lo standard nell'account e nella regione specificata. Ciò include la disabilitazione di tutti i controlli che si applicano allo standard. Per monitorare lo stato di queste attività, puoi controllare lo stato dello standard per l'account e la regione.

Comprendere i controlli di sicurezza in Security Hub CSPM

In AWS Security Hub CSPM, un controllo di sicurezza, noto anche come controllo, è una protezione all'interno di uno standard di sicurezza che aiuta un'organizzazione a proteggere la riservatezza, l'integrità e la disponibilità delle proprie informazioni. In Security Hub CSPM, un controllo è correlato a una risorsa specifica. AWS

Quando si abilita un controllo in uno o più standard, Security Hub CSPM inizia a eseguire i controlli di sicurezza su di esso. I controlli di sicurezza danno come risultato i risultati di Security Hub CSPM. Quando si disabilita un controllo, Security Hub CSPM interrompe l'esecuzione dei controlli di sicurezza su di esso e i risultati non vengono più generati.

È possibile abilitare o disabilitare i controlli singolarmente per un singolo account e. Regione AWS Per risparmiare tempo e ridurre la deriva della configurazione in ambienti con più account, consigliamo di utilizzare la configurazione centrale per abilitare o disabilitare i controlli. Con la configurazione centralizzata, l'amministratore delegato di Security Hub CSPM può creare policy che specificano come configurare un controllo su più account e regioni. Per ulteriori informazioni sull'attivazione e la disabilitazione dei controlli, vedere. Abilitazione dei controlli in Security Hub CSPM

Visualizzazione consolidata dei controlli

La pagina Controlli della console Security Hub CSPM mostra tutti i controlli disponibili nella versione corrente Regione AWS (puoi visualizzare i controlli nel contesto di uno standard visitando la pagina degli standard di sicurezza e scegliendo uno standard abilitato). Security Hub CSPM assegna ai controlli un ID, un titolo e una descrizione del controllo di sicurezza coerenti tra tutti gli standard. Gli ID dei controlli includono il numero pertinente Servizio AWS e univoco (ad esempio,). CodeBuild.3

Le seguenti informazioni sono disponibili nella pagina Controlli della console Security Hub CSPM:

- Un punteggio di sicurezza complessivo basato sulla percentuale di controlli superati rispetto al numero totale di controlli abilitati con dati
- Analisi degli stati di controllo in tutti i controlli CSPM di Security Hub supportati
- Il numero totale di controlli di sicurezza superati e non riusciti.
- Il numero di controlli di sicurezza non riusciti per controlli di diversa gravità e collegamenti per visualizzare ulteriori dettagli su tali controlli non riusciti.
- Un elenco di controlli CSPM di Security Hub, con filtri per visualizzare sottoinsiemi specifici di controlli.

Dalla pagina Controlli, puoi scegliere un controllo per visualizzarne i dettagli e agire sui risultati generati dal controllo. Da questa pagina, puoi anche abilitare o disabilitare un controllo di sicurezza nel tuo attuale Account AWS e Regione AWS. Le azioni di attivazione e disattivazione della pagina Controlli si applicano a tutti gli standard. Per ulteriori informazioni, consulta Abilitazione dei controlli in Security Hub CSPM.

Per gli account amministratore, la pagina Controlli riflette lo stato dei controlli negli account dei membri. Se un controllo di controllo ha esito negativo in almeno un account membro, lo stato del controllo è Non riuscito. Se hai impostato una regione di aggregazione, la pagina Controlli riflette lo stato dei controlli in tutte le regioni collegate. Se un controllo di controllo ha esito negativo in almeno una regione collegata, lo stato del controllo è Non riuscito.

La visualizzazione consolidata dei controlli causa modifiche ai campi di ricerca dei controlli nel AWS Security Finding Format (ASFF) che possono influire sui flussi di lavoro. Per ulteriori informazioni, consulta Visualizzazione consolidata dei controlli: modifiche ASFF.

Punteggio di sicurezza riepilogativo per i controlli

La pagina Controlli mostra un punteggio di sicurezza riepilogativo compreso tra 0 e 100 percento. Il punteggio di sicurezza riepilogativo viene calcolato in base alla percentuale di controlli superati rispetto al numero totale di controlli abilitati con dati relativi a tutti gli standard.

> **Note**
>
> Per visualizzare il punteggio di sicurezza complessivo dei controlli, devi aggiungere l'autorizzazione alla chiamata **`BatchGetControlEvaluations`** al ruolo IAM che utilizzi per accedere a Security Hub CSPM. Questa autorizzazione non è richiesta per visualizzare i punteggi di sicurezza per standard specifici.

Quando si abilita Security Hub CSPM, Security Hub CSPM calcola il punteggio di sicurezza iniziale entro 30 minuti dalla prima visita alla pagina di riepilogo o alla pagina degli standard di sicurezza sulla console Security Hub CSPM. Possono essere necessarie fino a 24 ore per la prima generazione dei punteggi di sicurezza nelle regioni della Cina e. AWS GovCloud (US) Regions

Oltre al punteggio di sicurezza complessivo, Security Hub CSPM calcola un punteggio di sicurezza standard per ogni standard abilitato entro 30 minuti dalla prima visita alla pagina di riepilogo o alla pagina degli standard di sicurezza. Per visualizzare un elenco degli standard attualmente abilitati, utilizza l'`GetEnabledStandards`operazione API.

AWS Config deve essere abilitato con la registrazione delle risorse per visualizzare le partiture. Per informazioni su come Security Hub CSPM calcola i punteggi di sicurezza, vedere. Calcolo dei punteggi di sicurezza

Dopo la prima generazione dei punteggi, Security Hub CSPM aggiorna i punteggi di sicurezza ogni 24 ore. Security Hub CSPM mostra un timestamp per indicare quando un punteggio di sicurezza è stato aggiornato l'ultima volta.

Se hai impostato una regione di aggregazione, il punteggio di sicurezza complessivo riflette i risultati del controllo nelle regioni collegate.

Riferimento di controllo per Security Hub CSPM

Questo riferimento di controllo fornisce una tabella dei controlli CSPM di AWS Security Hub disponibili con collegamenti a ulteriori informazioni su ciascun controllo. Nella tabella, i controlli sono elencati in ordine alfabetico per ID di controllo. Sono inclusi solo i controlli in uso attivo da Security Hub CSPM. I controlli ritirati sono esclusi dalla tabella.

La tabella fornisce le seguenti informazioni per ogni controllo:

- ID del controllo di sicurezza: questo ID si applica a tutti gli standard Servizio AWS e indica la risorsa e a cui si riferisce il controllo. La console Security Hub CSPM mostra gli ID di controllo di sicurezza, indipendentemente dal fatto che i risultati del controllo consolidato siano attivati o disattivati nel tuo account. Tuttavia, i risultati CSPM di Security Hub fanno riferimento agli ID di controllo di sicurezza solo se i risultati del controllo consolidato sono attivati nel tuo account. Se i risultati del controllo consolidato sono disattivati nel tuo account, alcuni ID di controllo variano in base allo standard dei risultati di controllo. Per una mappatura degli ID di controllo specifici degli standard agli ID dei controlli di sicurezza, consulta. In che modo il consolidamento influisce sugli ID e sui titoli di controllo

Se desideri configurare le automazioni per i controlli di sicurezza, ti consigliamo di filtrare in base all'ID del controllo anziché al titolo o alla descrizione. Sebbene Security Hub CSPM possa occasionalmente aggiornare i titoli o le descrizioni dei controlli, gli ID di controllo rimangono invariati.

I Control ID possono ignorare i numeri. Si tratta di segnaposti per controlli futuri.

- Titolo del controllo di sicurezza: questo titolo si applica a tutti gli standard. La console Security Hub CSPM mostra i titoli dei controlli di sicurezza, indipendentemente dal fatto che i risultati del controllo consolidato siano attivati o disattivati nel tuo account. Tuttavia, i risultati del CSPM di Security Hub fanno riferimento ai titoli di controllo di sicurezza solo se i risultati del controllo consolidato sono attivati nel tuo account. Se i risultati del controllo consolidato sono disattivati nel tuo account, alcuni titoli di controllo variano in base allo standard dei risultati di controllo. Per una mappatura degli ID di controllo specifici degli standard agli ID dei controlli di sicurezza, consulta. In che modo il consolidamento influisce sugli ID e sui titoli di controllo
- Standard applicabili: indica a quali standard si applica un controllo. Scegli un controllo per esaminare i requisiti specifici dei framework di conformità di terze parti.
- Severità: la severità di un controllo ne identifica l'importanza dal punto di vista della sicurezza. Per informazioni su come Security Hub CSPM determina la gravità del controllo, vedere. Livelli di gravità per i risultati del controllo
- Supporta parametri personalizzati: indica se il controllo supporta valori personalizzati per uno o più parametri. Scegliete un controllo per esaminare i dettagli dei parametri. Per ulteriori informazioni, consulta Comprensione dei parametri di controllo in Security Hub CSPM.
- Tipo di pianificazione: indica quando il controllo viene valutato. Per ulteriori informazioni, consulta Pianificazione dell'esecuzione dei controlli di sicurezza.

Scegli un controllo per esaminare ulteriori dettagli. I controlli sono elencati in ordine alfabetico in base all'ID del controllo di sicurezza.

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Account.1	Le informazioni di contatto relative alla sicurezza devono essere fornite per un Account AWS	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, migliori AWS pratiche di sicurezza di base v1.0.0 AWS , NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	No	Periodic (Periodico)
Account.2	Account AWS dovrebbe far parte di un' AWS Organizations organizzazione	NIST SP 800-53 Rev. 5, profilo CRI v2.2	HIGH (ELEVATO)	No	Periodic (Periodico)
ACM.1	I ACM-issued certificati importati devono essere rinnovati dopo un periodo di tempo specificato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	Sì	Modifica attivata e periodica
ACM.2	I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit	AWS Best practice di sicurezza di base v1.0.0, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO)	No	Modifica attivata
ACM.3	I certificati ACM devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Amplify.1	Le app Amplify devono essere taggate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Amplify.2	I rami Amplify devono essere etichettati	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
APIGateway.1	API Gateway REST e la registrazione dell'esecuzione delle WebSocket API devono essere abilitati	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	Sì	Modifica attivata
APIGateway.2	Le fasi dell'API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend.	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	MEDIO	No	Modifica attivata
APIGateway.3	Le fasi API REST di API Gateway devono avere AWS X-Ray la traccia abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	No	Modifica attivata
APIGateway.4	API Gateway deve essere associato a un ACL Web WAF	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
APIGateway.5	I dati della cache dell'API REST di API Gateway devono essere crittografati quando sono inattivi	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
APIGateway.8	Le rotte API Gateway devono specificare un tipo di autorizzazione	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊙ Sì	Periodic (Periodico)
APIGateway.9	La registrazione degli accessi deve essere configurata per API Gateway V2 Stages	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
APIGateway.10	Le integrazioni API Gateway V2 devono utilizzare HTTPS per le connessioni private	AWS Best practice di sicurezza di base v1.0.0	MEDIO	⊗ No	Modifica attivata
APIGateway.11	I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate	AWS Migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata
AppConfig.1	AWS AppConfig le applicazioni devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
AppConfig.2	AWS AppConfig i profili di configurazione devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
AppConfig.3	AWS AppConfig gli ambienti devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
AppConfig.4	AWS AppConfig le associazioni di estensioni devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
AppFlow.1	AppFlow I flussi Amazon devono essere etichettati	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
AppRunner.1	I servizi App Runner devono essere etichettati	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
AppRunner.2	I connettori VPC App Runner devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
AppSync.2	AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
AppSync.4	AWS AppSync Le API GraphQL devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
AppSync.5	AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	HIGH (ELEVATO	No	Modifica attivata
Athena.2	I cataloghi di dati Athena devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Athena.3	I gruppi di lavoro Athena devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Athena.4	I gruppi di lavoro Athena devono avere la registrazione abilitata	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	No	Modifica attivata
AutoScaling.1	I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB	AWS Best practice di sicurezza di base, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
AutoScaling.2	Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	Sì	Modifica attivata
AutoScaling.3	Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Modifica attivata
Autoscaling.5	Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici.	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Modifica attivata
AutoScaling.6	I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
AutoScaling.9	I gruppi di Auto Scaling di EC2 devono utilizzare i modelli di avvio EC2	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata
AutoScaling.10	I gruppi EC2 Auto Scaling devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Backup.1	AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	No	Modifica attivata
Backup.2	AWS Backup i punti di ripristino devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Backup.3	AWS Backup le casseforti devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Backup.4	AWS Backup i piani di report devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Backup.5	AWS Backup i piani di backup devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Batch.1	Le code di lavori in batch devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Batch.2	Le politiche di pianificazione dei batch devono essere contrassegnate	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
Batch.3	Gli ambienti di elaborazione in batch devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Batch.4	Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate.	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
Bedrock.1	Le fonti di dati Amazon Bedrock devono essere crittografate con chiavi gestite AWS KMS dal cliente	AWS Best practice di sicurezza di base	MEDIO	No	Modifica attivata
BedrockAgentCore.1	I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC	AWS Le migliori pratiche di sicurezza di base	HIGH (ELEVATO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
BedrockAgentCore.2	I AgentCore gateway Bedrock devono richiedere l'autorizzazione per le richieste in entrata	AWS Le migliori pratiche di sicurezza di base	HIGH (ELEVATO	⊗ No	Modifica attivata
BedrockAgentCore.3	Bedrock AgentCore Memory deve essere crittografata con chiavi gestite dal cliente AWS KMS	NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Modifica attivata
BedrockAgentCore.4	Bedrock AgentCore Gateway deve essere crittografato con chiavi gestite dal cliente AWS KMS	NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Modifica attivata
BedrockAgentCore.5	I browser AgentCore personalizzati Bedrock non devono utilizzare la modalità di rete pubblica	AWS Migliori pratiche di sicurezza di base	HIGH (ELEVATO	⊗ No	Modifica attivata
BedrockAgentCore.6	I browser AgentCore personalizzati Bedrock dovrebbero avere la registrazione della sessione abilitata	AWS Migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
BedrockAgentCore.7	Gli interpreti di codice AgentCore personalizzato Bedrock devono utilizzare una configurazione di rete privata	AWS Le migliori pratiche di sicurezza di base	HIGH (ELEVATO	No	Modifica attivata
CloudFormation.2	CloudFormation le pile devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
CloudFormation.3	CloudFormation gli stack dovrebbero avere la protezione dalla terminazione abilitata	AWS Migliori pratiche di sicurezza di base	MEDIO	No	Modifica attivata
CloudFormation.4	CloudFormation gli stack devono avere ruoli di servizio associati	AWS Migliori pratiche di sicurezza di base	MEDIO	No	Modifica attivata
CloudFront.1	CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudFront.3	CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
CloudFront.4	CloudFront le distribuzioni devono avere configurato il failover di origine	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	BASSO	⊗ No	Modifica attivata
CloudFront.5	CloudFront le distribuzioni dovrebbero avere la registrazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata
CloudFront.6	CloudFront le distribuzioni dovrebbero avere WAF abilitato	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudFront.7	CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata
CloudFront.8	CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	BASSO	⊗ No	Modifica attivata
CloudFront.9	CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
CloudFront.10	CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudFront.12	CloudFront le distribuzioni non devono puntare a origini S3 inesistenti	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO)	No	Periodic (Periodico)
CloudFront.13	CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine	AWS Buone pratiche di sicurezza di base v1.0.0, CRI Profile v2.2	MEDIO	No	Modifica attivata
CloudFront.14	CloudFront le distribuzioni devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
CloudFront.15	CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata	AWS Buone pratiche di sicurezza di base v1.0.0, CRI Profile v2.2	MEDIO	No	Modifica attivata
CloudFront.16	CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda	AWS Best practice di sicurezza di base v1.0.0	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudFront.17	CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati	AWS Best practice di sicurezza di base v1.0.0	MEDIO	⊗ No	Modifica attivata
CloudTrail.1	CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, AWS CRI Profile v2.2 AWS	HIGH (ELEVATO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudTrail.2	CloudTrail dovrebbe avere la crittografia a riposo abilitata	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.2.0, benchmark CIS AWS Foundations v1.4.0 Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, AWS NIST SP 800-171 Rev. 2, AWS PCI DSS v3.2.1, PCI DSS v4.0.1, profilo CRI v4.0.1 2.2	MEDIO	⊗ No	Periodic (Periodico)
CloudTrail.3	Almeno una CloudTrail traccia deve essere abilitata	NIST SP 800-171 Rev. 2, PCI DSS versione 4.0.1, PCI DSS versione 3.2.1, profilo CRI versione 2.2	HIGH (ELEVATO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudTrail.4	CloudTrail la convalida dei file di registro deve essere abilitata	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.4.0, benchmark CIS AWS Foundations AWS v1.2.0, Best practice di sicurezza di base v1.0.0, NIST SP 800-53 AWS Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudTrail.5	CloudTrail i trail devono essere integrati con Amazon CloudWatch Logs	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0, migliori pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5 AWS , PCI DSS v3.2.1, PCI DSS v4.0.1, profilo AWS CRI v2.2	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudTrail.6	Assicurati che il bucket S3 utilizzato per archiviare CloudTrail i log non sia accessibile al pubblico	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0, PCI AWS DSS v4.0.1, profilo CRI v2.2	CRITICO	No	Modifica attivata e periodica
CloudTrail.7	Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0, benchmark CIS AWS Foundations v3.0.0, PCI DSS v4.0.1, profilo AWS CRI v2.2 AWS	BASSO	No	Periodic (Periodico)
CloudTrail.9	CloudTrail i sentieri devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
CloudTrail.10	CloudTrail Gli archivi dati di Lake Event devono essere crittografati con Customer Managed AWS KMS keys	NIST SP 800-53 Rev. 5	MEDIO	Sì	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudWatch.1	Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudWatch.2	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle chiamate API non autorizzate	Benchmark CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudWatch.3	Verifica se esistono un filtro e un allarme per le metriche dei log per l'accesso alla Console di gestione senza autenticazione a più fattori (MFA)	Benchmark CIS AWS Foundations v1.2.0, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudWatch.4	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle policy IAM	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudWatch.5	Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrail alla configurazione	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudWatch.6	Assicurati che esistano un filtro metrico di registro e un allarme per gli errori di Console di gestione AWS autenticazione	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudWatch.7	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alla disabilitazione o all'eliminazione pianificata delle chiavi gestite dal cliente (CMK) create dal cliente	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudWatch.8	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle policy dei bucket S3	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudWatch.9	Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche AWS Config alla configurazione	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudWatch.10	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate al gruppo di sicurezza	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudWatch.11	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle liste di controllo degli accessi alla rete (NACL)	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudWatch.12	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ai gateway di rete	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudWatch.13	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle tabelle di routing	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudWatch.14	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate al VPC	Benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
CloudWatch.15	CloudWatch gli allarmi dovrebbero avere azioni specificate configurate	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, profilo CRI v2.2	HIGH (ELEVATO	✓ Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudWatch.16	CloudWatch i gruppi di log devono essere conservati per un periodo di tempo specificato	NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	Sì	Periodic (Periodico)
CloudWatch.17	CloudWatch le azioni di allarme devono essere abilitate	NIST SP 800-53 Rev. 5, profilo CRI v2.2	HIGH (ELEVATO	No	Modifica attivata
CodeArtifact.1	CodeArtifact i repository devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
CodeBuild.1	CodeBuild Gli URL del repository di origine Bitbucket non devono contenere credenziali riservate	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	CRITICO	No	Modifica attivata
CodeBuild.2	CodeBuild le variabili di ambiente del progetto non devono contenere credenziali di testo non crittografato	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	CRITICO	No	Modifica attivata
CodeBuild.3	CodeBuild I log S3 devono essere crittografati	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	BASSO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CodeBuild.4	CodeBuild gli ambienti di progetto devono avere una configurazione di registrazione	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	No	Modifica attivata
CodeBuild.7	CodeBuild Le esportazioni dei gruppi di report devono essere crittografate quando sono inattive	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	No	Modifica attivata
CodeGuruProfiler.1	CodeGuru I gruppi di profilazione di Profiler devono essere etichettati	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
CodeGuruReviewer.1	CodeGuru Le associazioni dei repository dei revisori devono essere etichettate	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Cognito.1	I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard	AWS Le migliori pratiche di sicurezza di base	MEDIO	Sì	Modifica attivata
Cognito.2	I pool di identità di Cognito non dovrebbero consentire identità non autenticate	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	No	Modifica attivata
Cognito.3	Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	Sì	Modifica attivata
Cognito.4	I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata	AWS Le migliori pratiche di sicurezza di base	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Cognito.5	La MFA deve essere abilitata per i pool di utenti di Cognito	AWS Migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata
Cognito.6	I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata	AWS Le migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata
Config.1	AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse	Benchmark CIS AWS Foundations v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, benchmark AWS CIS Foundations v1.2.0, Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, AWS PCI DSS v3.2.1, CRI Profile v2.2 AWS	CRITICO	⊙ Sì	Periodic (Periodico)
Connect.1	I tipi di oggetto Connect Customer Customer Profiles devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Connect.2	Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	No	Modifica attivata
DataFirehose.1	I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)
DataSync.1	DataSync le attività dovrebbero avere la registrazione abilitata	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	No	Modifica attivata
DataSync.2	DataSync le attività devono essere etichettate	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
Detective.1	I grafici del comportamento dei Detective devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
DMS.1	Le istanze di replica del Database Migration Service non devono essere pubbliche	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	CRITICO	No	Periodic (Periodico)
DMS.2	I certificati DMS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
DMS.3	Le sottoscrizioni agli eventi DMS devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
DMS.4	Le istanze di replica DMS devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
DMS.5	I sottoreti di replica DMS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
DMS.6	L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Modifica attivata
DMS.7	Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Modifica attivata
DMS.8	Le attività di replica DMS per il database di origine devono avere la registrazione abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
DMS.9	Gli endpoint DMS devono utilizzare SSL	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
DMS.10	Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
DMS.11	Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
DMS.12	Gli endpoint DMS per Redis OSS devono avere TLS abilitato	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
DMS.13	Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità	AWS Best practice di sicurezza di base	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
DocumentDB.1	I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata
DocumentDB.2	I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	Sì	Modifica attivata
DocumentDB.3	Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	CRITICO	No	Modifica attivata
DocumentDB.4	I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Modifica attivata
DocumentDB.5	I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
DocumentDB.6	I cluster Amazon DocumentDB devono essere crittografati in transito	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
DynamoDB.1	Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊙ Sì	Periodic (Periodico)
DynamoDB.2	Le tabelle DynamoDB devono avere il ripristino point-in-time abilitato	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
DynamoDB.3	I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
DynamoDB.4	Le tabelle DynamoDB devono essere presenti in un piano di backup	NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊙ Sì	Periodic (Periodico)
DynamoDB.5	Le tabelle DynamoDB devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
DynamoDB 6	Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata
DynamoDB 7	I cluster DynamoDB Accelerator devono essere crittografati in transito	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
EC2.1	Le istantanee EBS non devono essere ripristinabili pubblicamente	AWS Best practice di sicurezza di base v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, profilo CRI v2.2	CRITICO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.2	I gruppi di sicurezza VPC predefiniti non devono consentire il traffico in entrata o in uscita	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.2.0, best practice di sicurezza di base v1.0.0, PCI DSS v3.2.1, benchmark AWS CIS Foundations AWS v1.4.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2 AWS	HIGH (ELEVATO)	⊗ No	Modifica attivata
EC2.3	I volumi EBS collegati devono essere crittografati quando sono inattivi	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
EC2.4	Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊙ Sì	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.6	La registrazione del flusso VPC deve essere abilitata in tutti i VPC	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.2.0, best practice di sicurezza di base v1.0.0, PCI DSS v3.2.1, benchmark AWS CIS Foundations AWS v1.4.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, profilo CRI v2.2 AWS	MEDIO	⊗ No	Periodic (Periodico)
EC2.7	La crittografia predefinita di EBS deve essere abilitata	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, migliori pratiche di sicurezza di base v1.0.0 AWS , benchmark AWS CIS Foundations v1.4.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2 AWS	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.8	Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)	Benchmark CIS AWS Foundations v5.0.0, CIS Foundations Benchmark v3.0.0, migliori pratiche di sicurezza di base, NIST SP 800-53 Rev. 5 AWS , PCI DSS v4.0.1, AWS CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Modifica attivata
EC2.9	Le istanze EC2 non devono avere un indirizzo IPv4 pubblico	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Modifica attivata
EC2.10	Amazon EC2 deve essere configurato per utilizzare endpoint VPC creati per il servizio Amazon EC2.	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
EC2.12	Le EIP EC2 non utilizzate devono essere rimosse	PCI DSS versione 3.2.1, NIST SP 800-53 Rev. 5, profilo CRI versione 2.2	BASSO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.13	I gruppi di sicurezza non dovrebbero consentire l'accesso da 0.0.0. 0/0 o: :/0 alla porta 22	Benchmark CIS AWS Foundations versione 1.2.0, PCI DSS versione 3.2.1, PCI DSS versione 4.0.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, profilo CRI versione 2.2	HIGH (ELEVATO	⊗ No	Modifica attivata e periodica
EC2.14	I gruppi di sicurezza non dovrebbero consentire l'accesso a partire dalla versione 0.0.0. 0/0 o: :/0 alla porta 3389	Benchmark CIS AWS Foundations versione 1.2.0, PCI DSS versione 4.0.1, profilo CRI versione 2.2	HIGH (ELEVATO	⊗ No	Modifica attivata e periodica
EC2.15	Le sottoreti EC2 non devono assegnare automaticamente indirizzi IP pubblici	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
EC2.16	Gli elenchi di controllo degli accessi alla rete non utilizzati devono essere rimossi	AWS Migliori pratiche di sicurezza di base, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.17	Le istanze EC2 non devono utilizzare più ENI	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata
EC2.18	I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	HIGH (ELEVATO	⊙ Sì	Modifica attivata
EC2.19	I gruppi di sicurezza non dovrebbero consentire l'accesso illimitato alle porte ad alto rischio	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	CRITICO	⊗ No	Modifica attivata e periodica
EC2.20	Entrambi i tunnel VPN per una connessione AWS Site-to-Site VPN dovrebbero essere attivi	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.21	Gli ACL di rete non dovrebbero consentire l'accesso a partire dalla versione 0.0.0.0/0 alla porta 22 o alla porta 3389	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Best practice di sicurezza di base, NIST SP AWS 800-53 Rev. 5, NIST SP 800-171 Rev. 2 AWS , PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
EC2.22	I gruppi di sicurezza EC2 non utilizzati devono essere rimossi	Profilo CRI v2.2	MEDIO	⊗ No	Periodic (Periodico)
EC2.23	I gateway di transito EC2 non dovrebbero accettare automaticamente le richieste di allegati VPC	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	HIGH (ELEVATO	⊗ No	Modifica attivata
EC2.24	I tipi di istanze paravirtuali EC2 non devono essere utilizzati	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.25	I modelli di lancio EC2 non devono assegnare IP pubblici alle interfacce di rete	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Modifica attivata
EC2.28	I volumi EBS devono essere inclusi in un piano di backup	NIST SP 800-53 Rev. 5, profilo CRI v2.2	BASSO	Sì	Periodic (Periodico)
EC2.33	Gli allegati del gateway di transito EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.34	Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.35	Le interfacce di rete EC2 devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.36	I gateway per i clienti EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.37	Gli indirizzi IP elastici EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.38	Le istanze EC2 devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.39	I gateway Internet EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.40	I gateway NAT EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.41	Gli ACL di rete EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.42	Le tabelle delle rotte EC2 devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.43	I gruppi di sicurezza EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.44	Le sottoreti EC2 devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.45	I volumi EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.46	I VPC Amazon devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.47	I servizi endpoint Amazon VPC devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.48	I log di flusso di Amazon VPC devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.49	Le connessioni peering Amazon VPC devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.50	I gateway VPN EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.51	Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	BASSO	No	Modifica attivata
EC2.52	I gateway di transito EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.53	I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, PCI DSS AWS v4.0.1, profilo CRI v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
EC2.54	I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione del server remoto	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, PCI DSS AWS v4.0.1, profilo CRI v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
EC2.55	I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	Sì	Periodic (Periodico)
EC2.56	I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	Sì	Periodic (Periodico)
EC2.57	I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	Sì	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.58	I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	Sì	Periodic (Periodico)
EC2.60	I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager.	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	Sì	Periodic (Periodico)
EC2.170	I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	BASSO	No	Modifica attivata
EC2.171	Le connessioni VPN EC2 devono avere la registrazione abilitata	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Modifica attivata
EC2.172	Le impostazioni VPC Block Public Access di EC2 dovrebbero bloccare il traffico del gateway Internet	AWS Le migliori pratiche di sicurezza di base	MEDIO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.173	Le richieste Spot Fleet di EC2 con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	No	Modifica attivata
EC2.174	I set di opzioni DHCP EC2 devono essere etichettati	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
EC2.175	I modelli di lancio di EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.176	Gli elenchi di prefissi EC2 devono essere etichettati	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
EC2.177	Le sessioni Traffic Mirror di EC2 devono essere contrassegnate	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
EC2.178	I filtri Traffic Mirror di EC2 devono essere etichettati	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
EC2.179	Gli obiettivi del Traffic Mirror di EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.180	Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination	AWS Buone pratiche di sicurezza di base v1.0.0, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
EC2.181	I modelli di lancio EC2 devono abilitare la crittografia per i volumi EBS collegati	AWS Best practice di sicurezza di base v1.0.0, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
EC2.182	Le istantanee EBS non devono essere accessibili al pubblico	AWS Migliori pratiche di sicurezza di base	HIGH (ELEVATO	⊗ No	Modifica attivata
EC2.183	Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2	AWS Migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata
ECR.1	Gli archivi privati ECR devono avere la scansione delle immagini configurata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, profilo CRI v2.2	HIGH (ELEVATO	⊗ No	Periodic (Periodico)
ECR.2	Gli archivi privati ECR devono avere l'immutabilità dei tag configurata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ECR.3	Gli archivi ECR devono avere almeno una politica del ciclo di vita configurata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ECR.4	Gli archivi pubblici ECR devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata
ECR.5	Gli archivi ECR devono essere crittografati e gestiti dal cliente AWS KMS keys	NIST SP 800-53 Rev. 5	MEDIO	⊙ Sì	Modifica attivata
ECS.2	Ai servizi ECS non dovrebbero essere assegnati automaticamente indirizzi IP pubblici	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Modifica attivata
ECS.3	Le definizioni delle attività ECS non devono condividere lo spazio dei nomi del processo dell'host	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Modifica attivata
ECS.4	I contenitori ECS devono essere eseguiti come non privilegiati	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	HIGH (ELEVATO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ECS.5	I contenitori ECS devono essere limitati all'accesso in sola lettura ai filesystem root	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	HIGH (ELEVATO	No	Modifica attivata
ECS.8	I segreti non devono essere passati come variabili di ambiente del contenitore	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Modifica attivata
ECS.9	Le definizioni delle attività ECS devono avere una configurazione di registrazione	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	HIGH (ELEVATO	No	Modifica attivata
ECS.10	I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Modifica attivata
ECS.12	I cluster ECS devono utilizzare Container Insights	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata
ECS.13	I servizi ECS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ECS.14	I cluster ECS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	✓ Sì	Modifica attivata
ECS.15	Le definizioni delle attività ECS devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	✓ Sì	Modifica attivata
ECS.16	I set di attività ECS non devono assegnare automaticamente indirizzi IP pubblici	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	✗ No	Modifica attivata
ECS.17	Le definizioni delle attività ECS non devono utilizzare la modalità di rete host	NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	✗ No	Modifica attivata
ECS.18	Le definizioni delle attività ECS devono utilizzare la crittografia in transito per i volumi EFS	AWS Best practice di sicurezza di base	MEDIO	✗ No	Modifica attivata
ECS.19	I fornitori di capacità ECS dovrebbero avere abilitato la protezione gestita dalla terminazione	AWS Le migliori pratiche di sicurezza di base	MEDIO	✗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ECS.20	Le definizioni delle attività ECS devono configurare gli utenti non root nelle definizioni dei contenitori Linux	AWS Le migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata
ECS.21	Le definizioni delle attività ECS devono configurare gli utenti non amministratori nelle definizioni dei contenitori Windows	AWS Best practice di sicurezza di base	MEDIO	⊗ No	Modifica attivata
EFS.1	Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, migliori AWS pratiche di sicurezza di base v1.0.0 AWS , NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Periodic (Periodico)
EFS.2	I volumi Amazon EFS devono essere inclusi nei piani di backup	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EFS.3	I punti di accesso EFS devono applicare una directory principale	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
EFS.4	I punti di accesso EFS devono applicare un'identità utente	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
EFS.5	I punti di accesso EFS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata
EFS.6	Gli obiettivi di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, profilo CRI v2.2	MEDIO	⊗ No	Periodic (Periodico)
EFS.7	I file system EFS devono avere i backup automatici abilitati	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EFS.8	I file system EFS devono essere crittografati quando sono inattivi	CIS AWS Foundations Benchmark v5.0.0, migliori pratiche di sicurezza di AWS base, profilo CRI v2.2	MEDIO	Sì	Modifica attivata
EKS.1	Gli endpoint del cluster EKS non devono essere accessibili al pubblico	AWS Migliori pratiche di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
EKS.2	I cluster EKS devono essere eseguiti su una versione di Kubernetes supportata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Modifica attivata
EKS.6	I cluster EKS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EKS.7	Le configurazioni dei provider di identità EKS devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EKS.8	I cluster EKS dovrebbero avere la registrazione di controllo abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EKS.9	I gruppi di nodi EKS devono essere eseguiti su una versione di Kubernetes supportata	AWS Best practice di sicurezza di base	HIGH (ELEVATO	No	Modifica attivata
ElastiCache.1	ElastiCache I cluster (Redis OSS) devono avere i backup automatici abilitati	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	HIGH (ELEVATO	Sì	Periodic (Periodico)
ElastiCache.2	ElastiCache i cluster dovrebbero avere gli aggiornamenti automatici delle versioni minori abilitati	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
ElastiCache.3	ElastiCache i gruppi di replica devono avere il failover automatico abilitato	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)
ElastiCache.4	ElastiCache i gruppi di replica devono essere crittografati a riposo	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ElastiCache.5	ElastiCache i gruppi di replica devono essere crittografati in transito	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)
ElastiCache.6	ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)
ElastiCache.7	ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
ElasticBeanstalk.1	Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	No	Modifica attivata
ElasticBeanstalk.2	Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ElasticBeanstalk.3	Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	Sì	Modifica attivata
ELB.1	Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS	AWS Best practice di sicurezza di base v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)
ELB.2	I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	MEDIO	No	Modifica attivata
ELB.3	I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ELB.4	Application Load Balancer deve essere configurato per eliminare le intestazioni http	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ELB.5	La registrazione di Application e Classic Load Balancers deve essere abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ELB.6	Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ELB.7	I Classic Load Balancer dovrebbero avere abilitato il drenaggio della connessione	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata
ELB.8	I sistemi Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una configurazione avanzata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ELB.9	I sistemi Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ELB.10	Classic Load Balancer dovrebbe estenders i su più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊙ Sì	Modifica attivata
ELB.12	Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa.	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ELB.13	I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊙ Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ELB.14	Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa.	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ELB.16	Gli Application Load Balancer devono essere associati a un AWS ACL web WAF	NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata
ELB.17	Gli Application e Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ELB.18	I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito	AWS Best practice di sicurezza di base v1.0.0, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ELB.21	I gruppi target di Application e Network Load Balancer devono utilizzare protocolli di controllo dello stato crittografati	AWS Buone pratiche di sicurezza di base v1.0.0, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ELB.22	I gruppi bersaglio dell'ELB devono utilizzare protocolli di trasporto criptati	AWS Buone pratiche di sicurezza di base v1.0.0, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
EMR.1	I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO)	⊗ No	Periodic (Periodico)
EMR.2	L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	CRITICO	⊗ No	Periodic (Periodico)
EMR.3	Le configurazioni di sicurezza di Amazon EMR devono essere crittografate quando sono inattive	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EMR.4	Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ES.1	I domini Elasticsearch devono avere la crittografia a riposo abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Periodic (Periodico)
ES.2	I domini Elasticsearch non dovrebbero essere accessibili al pubblico	AWS Best practice di sicurezza di base, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, CRI Profile v2.2	CRITICO	⊗ No	Periodic (Periodico)
ES.3	I domini Elasticsearch devono crittografare i dati inviati tra i nodi	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ES.4	La registrazione degli errori del dominio Elasticsearch nei registri deve essere abilitata CloudWatch	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ES.5	I domini Elasticsearch devono avere la registrazione di controllo abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ES.6	I domini Elasticsearch devono avere almeno tre nodi di dati	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ES.7	I domini Elasticsearch devono essere configurati con almeno tre nodi master dedicati	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ES.8	Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
ES.9	I domini Elasticsearch devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	✓ Sì	Modifica attivata
EventBridge.2	EventBridge i bus degli eventi devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	✓ Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EventBridge.3	EventBridge i bus di eventi personalizzati devono avere una politica basata sulle risorse allegata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	BASSO	No	Modifica attivata
EventBridge.4	EventBridge gli endpoint globali dovrebbero avere la replica degli eventi abilitata	NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	No	Modifica attivata
FraudDetector.1	I tipi di entità Amazon Fraud Detector devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
FraudDetector.2	Le etichette di Amazon Fraud Detector devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
FraudDetector.3	I risultati di Amazon Fraud Detector devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
FraudDetector.4	Le variabili di Amazon Fraud Detector devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
FSx.1	I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	⊗ No	Periodic (Periodico)
FSx.2	I file system FSx for Lustre devono essere configurati per copiare i tag nei backup	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	⊗ No	Periodic (Periodico)
FSx.3	I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
FSx.4	I file system FSx for NetApp ONTAP devono essere configurati per l'implementazione Multi-AZ	AWS Best practice di sicurezza di base	MEDIO	✓ Sì	Periodic (Periodico)
FSx.5	I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
Glue.1	AWS Glue i lavori devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	✓ Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Glue.3	AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inattive	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
Glue.4	AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
GlobalAccelerator.1	Gli acceleratori Global Accelerator devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata
GuardDuty.1	GuardDuty dovrebbe essere abilitato	AWS Best practice di sicurezza di base, 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 (ELEVATO	⊗ No	Periodic (Periodico)
GuardDuty.2	GuardDuty i filtri devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata
GuardDuty.3	GuardDuty Gli IPset devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
GuardDuty.4	GuardDuty i rilevatori devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
GuardDuty.5	GuardDuty EKS Audit Log Monitoring deve essere abilitato	AWS Best practice di sicurezza di base, CRI Profile v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
GuardDuty.6	GuardDuty La protezione Lambda deve essere abilitata	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
GuardDuty.7	GuardDuty EKS Runtime Monitoring deve essere abilitato	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
GuardDuty.8	GuardDuty La protezione da malware per EC2 deve essere abilitata	AWS Best practice di sicurezza di base, CRI Profile v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
GuardDuty.9	GuardDuty La protezione RDS deve essere abilitata	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
GuardDuty.10	GuardDuty La protezione S3 deve essere abilitata	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
GuardDuty.11	GuardDuty Il monitoraggio del runtime deve essere abilitato	AWS Best practice di sicurezza di base, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Periodic (Periodico)
GuardDuty.12	GuardDuty Il monitoraggio del runtime ECS deve essere abilitato	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
GuardDuty.13	GuardDuty Il monitoraggio del runtime EC2 deve essere abilitato	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
IAM.1	Le politiche IAM non dovrebbero consentire privilegi amministrativi completi «*»	Benchmark CIS AWS Foundations v1.2.0, migliori pratiche di sicurezza di base v1.0.0, PCI DSS v3.2.1, benchmark CIS AWS Foundations v1.4.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 AWS Rev. 2, profilo CRI v2.2	HIGH (ELEVATO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.2	Gli utenti IAM non devono avere policy IAM allegate	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.2.0, best practice di sicurezza di base v1.0.0, PCI AWS DSS v3.2.1, NIST SP 800-53 Rev. 5 AWS , NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Modifica attivata
IAM.3	Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno	Benchmark CIS AWS Foundations v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, benchmark AWS CIS Foundations v1.2.0, Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, AWS PCI DSS v4.0.1, CRI Profile v2.2 AWS	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.4	La chiave di accesso utente root IAM non dovrebbe esistere	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, Best AWS practice di sicurezza di base v1.0.0, PCI DSS v3.2.1, AWS NIST SP 800-53 Rev. 5, CRI Profile AWS v2.2	CRITICO	⊗ No	Periodic (Periodico)
IAM.5	L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console.	Benchmark CIS AWS Foundations v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, benchmark AWS CIS Foundations v1.2.0, Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, AWS PCI DSS v4.0.1, CRI Profile v2.2 AWS	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.6	La MFA hardware deve essere abilitata per l'utente root	Benchmark CIS AWS Foundations v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, benchmark AWS CIS Foundations AWS v1.2.0, Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, AWS PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	CRITICO	⊗ No	Periodic (Periodico)
IAM.7	Le politiche relative alle password per gli utenti IAM dovrebbero avere configurazioni solide	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊙ Sì	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.8	Le credenziali utente IAM non utilizzate devono essere rimosse	Benchmark CIS AWS Foundations v1.2.0, migliori pratiche di sicurezza di AWS base, 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	MEDIO	⊗ No	Periodic (Periodico)
IAM.9	L'MFA deve essere abilitata per l'utente root	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, AWS PCI DSS v4.0.1, Profilo CRI v2.2	CRITICO	⊗ No	Periodic (Periodico)
IAM.10	Le politiche relative alle password per gli utenti IAM dovrebbero avere configurazioni solide	NIST SP 800-171 Rev. 2, PCI DSS versione 3.2.1, profilo CRI versione 2.2	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.11	Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola	Benchmark CIS AWS Foundations versione 1.2.0, NIST SP 800-171 Rev. 2, PCI DSS versione 4.0.1, profilo CRI versione 2.2	MEDIO	⊗ No	Periodic (Periodico)
IAM.12	Assicurati che la politica delle password IAM richieda almeno una lettera minuscola	Benchmark CIS AWS Foundations versione 1.2.0, NIST SP 800-171 Rev. 2, PCI DSS versione 4.0.1, profilo CRI versione 2.2	MEDIO	⊗ No	Periodic (Periodico)
IAM.13	Assicurati che la politica delle password IAM richieda almeno un simbolo	Benchmark CIS AWS Foundations v1.2.0, NIST SP 800-171 Rev. 2, profilo CRI v2.2	MEDIO	⊗ No	Periodic (Periodico)
IAM.14	Assicurati che la politica delle password IAM richieda almeno un numero	Benchmark CIS AWS Foundations versione 1.2.0, NIST SP 800-171 Rev. 2, PCI DSS versione 4.0.1, profilo CRI versione 2.2	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.15	Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, profilo CRI v2.2 AWS	MEDIO	⊗ No	Periodic (Periodico)
IAM.16	Verifica che la policy delle password di IAM impedisca il riutilizzo delle password	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, profilo AWS CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
IAM.17	Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno	Benchmark CIS AWS Foundations versione 1.2.0, PCI DSS versione 4.0.1, profilo CRI versione 2.2	BASSO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.18	Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, profilo AWS CRI v2.2	BASSO	⊗ No	Periodic (Periodico)
IAM.19	L'MFA deve essere abilitata per tutti gli utenti IAM	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS versione 3.2.1, PCI DSS versione 4.0.1, profilo CRI versione 2.2	MEDIO	⊗ No	Periodic (Periodico)
IAM.21	Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.22	Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.4.0, NIST SP 800-171 Rev. 2, profilo CRI AWS v2.2	MEDIO	No	Periodic (Periodico)
IAM.23	Gli analizzatori IAM Access Analyzer devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IAM.24	I ruoli IAM devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IAM.25	Gli utenti IAM devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IAM.26	SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, profilo CRI AWS v2.2	MEDIO	No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.27	Le identità IAM non dovrebbero avere la AWSCloudShellFullAccess policy allegata	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, profilo CRI AWS v2.2	MEDIO	⊗ No	Modifica attivata
IAM.28	L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, profilo CRI AWS v2.2	HIGH (ELEVATO	⊗ No	Periodic (Periodico)
Inspector.1	La scansione di Amazon Inspector EC2 deve essere abilitata	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Periodic (Periodico)
Inspector.2	La scansione ECR di Amazon Inspector deve essere abilitata	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Periodic (Periodico)
Inspector.3	La scansione del codice Amazon Inspector Lambda deve essere abilitata	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Periodic (Periodico)
Inspector.4	La scansione standard di Amazon Inspector Lambda deve essere abilitata	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IoT.1	AWS IoT Device Defender i profili di sicurezza devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoT.2	AWS IoT Core le azioni di mitigazione devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoT.3	AWS IoT Core le dimensioni devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoT.4	AWS IoT Core gli autorizzatori devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoT.5	AWS IoT Core gli alias di ruolo devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoT.6	AWS IoT Core le politiche devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoTSiteWise.1	AWS IoT SiteWise i modelli di asset devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IoTSiteWise.2	AWS IoT SiteWise i dashboard devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoTSiteWise.3	AWS IoT SiteWise i gateway devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoTSiteWise.4	AWS IoT SiteWise i portali devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoTSiteWise.5	AWS IoT SiteWise i progetti devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoTTwinMaker.1	AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoTTwinMaker.2	AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
IoTTwinMaker.3	AWS TwinMaker Le scene IoT devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoTTwinMaker.4	AWS TwinMaker Le entità IoT devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IoTWireless.1	AWS I gruppi multicast IoT Wireless devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoTWireless.2	AWS I profili dei servizi IoT Wireless devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoTWireless.3	AWS Le attività IOT Wireless FUOTA devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IVS.1	Le coppie di chiavi di riproduzione IVS devono essere etichettate	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
IVS.2	Le configurazioni di registrazione IVS devono essere contrassegnate	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
IVS.3	I canali IVS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Keyspaces.1	Gli spazi chiave di Amazon Keyspaces devono essere etichettati	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Kinesis.1	Gli stream Kinesis devono essere crittografati quando sono inattivi	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata
Kinesis.2	Gli stream Kinesis devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Kinesis.3	I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato	AWS Le migliori pratiche di sicurezza di base	MEDIO	Sì	Modifica attivata
KMS.1	Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata
KMS.2	I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata
KMS.3	AWS KMS keys non deve essere eliminato involontariamente	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	CRITICO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
KMS.4	AWS KMS key la rotazione dovrebbe essere abilitata	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.4.0, benchmark CIS Foundations v1.2.0, AWS NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, AWS PCI DSS v4.0.1, Profilo CRI v2.2	MEDIO	⊗ No	Periodic (Periodico)
KMS.5	Le chiavi KMS non devono essere accessibili al pubblico	AWS Best practice di sicurezza di base, CRI Profile v2.2	CRITICO	⊗ No	Modifica attivata
Lambda.1	Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	CRITICO	⊗ No	Modifica attivata
Lambda.2	Le funzioni Lambda devono utilizzare runtime supportati	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Lambda.3	Le funzioni Lambda devono trovarsi in un VPC	PCI DSS versione 3.2.1, NIST SP 800-53 Rev. 5, profilo CRI versione 2.2	BASSO	⊗ No	Modifica attivata
Lambda.5	Le funzioni VPC Lambda devono funzionare in più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	✓ Sì	Modifica attivata
Lambda.6	Le funzioni Lambda devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	✓ Sì	Modifica attivata
Lambda.7	Le funzioni Lambda devono avere la traccia AWS X-Ray attiva abilitata	NIST SP 800-53 Rev. 5, profilo CRI v2.2	BASSO	⊗ No	Modifica attivata
Macie.1	Amazon Macie dovrebbe essere abilitato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Periodic (Periodico)
Macie.2	Il rilevamento automatico dei dati sensibili di Macie dovrebbe essere abilitato	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	HIGH (ELEVATO)	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
MSK.1	I cluster MSK devono essere crittografati durante il transito tra i nodi del broker	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
MSK.2	I cluster MSK dovrebbero avere configurato un monitoraggio avanzato	NIST SP 800-53 Rev. 5, profilo CRI v2.2	BASSO	⊗ No	Modifica attivata
MSK.3	I connettori MSK Connect devono essere crittografati in transito	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
MSK.4	L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato	AWS Migliori pratiche di sicurezza di base, CRI Profile v2.2	CRITICO	⊗ No	Modifica attivata
MSK.5	I connettori MSK dovrebbero avere la registrazione abilitata	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
MSK.6	I cluster MSK devono disabilitare l'accesso non autenticato	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
MQ.2	I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch	AWS Migliori pratiche di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
MQ.4	I broker Amazon MQ devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata
MQ.5	I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby	NIST SP 800-53 Rev. 5, profilo CRI v2.2	BASSO	⊗ No	Modifica attivata
MQ.6	I broker RabbitMQ devono utilizzare la modalità di distribuzione cluster	NIST SP 800-53 Rev. 5, profilo CRI v2.2	BASSO	⊗ No	Modifica attivata
Neptune.1	I cluster Neptune DB devono essere crittografati a riposo	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
Neptune.2	I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Neptune.3	Le istantanee del cluster Neptune DB non devono essere pubbliche	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	CRITICO	⊗ No	Modifica attivata
Neptune.4	I cluster Neptune DB devono avere la protezione da eliminazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	BASSO	⊗ No	Modifica attivata
Neptune.5	I cluster Neptune DB devono avere i backup automatici abilitati	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊘ Sì	Modifica attivata
Neptune.6	Le istantanee del cluster Neptune DB devono essere crittografate a riposo	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
Neptune.7	I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Neptune.8	I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee.	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata
Neptune.9	I cluster Neptune DB devono essere distribuiti su più zone di disponibilità	NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata
NetworkFirewall.1	I firewall Network Firewall devono essere implementati su più zone di disponibilità	NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata
NetworkFirewall.2	La registrazione del Network Firewall deve essere abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
NetworkFirewall.3	Le policy del Network Firewall devono avere almeno un gruppo di regole associato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
NetworkFirewall.4	L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere «drop or forward» per pacchetti completi.	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata
NetworkFirewall.5	L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati.	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	MEDIO	No	Modifica attivata
NetworkFirewall.6	Il gruppo di regole del firewall di rete stateless non deve essere vuoto	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	MEDIO	No	Modifica attivata
NetworkFirewall.7	I firewall Network Firewall devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
NetworkFirewall.8	Le politiche firewall del Network Firewall devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
NetworkFirewall.9	I firewall Network Firewall devono avere la protezione da eliminazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata
NetworkFirewall.10	I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
Opensearch.1	OpenSearch i domini devono avere la crittografia a riposo abilitata	AWS Best practice di sicurezza di base v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
Opensearch.2	OpenSearch i domini non dovrebbero essere accessibili al pubblico	AWS Buone pratiche di sicurezza di base v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI Profile v2.2	CRITICO	⊗ No	Modifica attivata
Opensearch.3	OpenSearch i domini devono crittografare i dati inviati tra i nodi	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Opensearch.4	OpenSearch la registrazione degli errori di dominio nei CloudWatch registri dovrebbe essere abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata
Opensearch.5	OpenSearch i domini devono avere la registrazione di controllo abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
Opensearch.6	OpenSearch i domini devono avere almeno tre nodi di dati	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
Opensearch.7	OpenSearch i domini devono avere un controllo granulare degli accessi abilitato	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Modifica attivata
Opensearch.8	Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Opensearch.9	OpenSearch i domini devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	✓ Sì	Modifica attivata
Opensearch.10	OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	✗ No	Modifica attivata
Opensearch.11	OpenSearch i domini devono avere almeno tre nodi primari dedicati	NIST SP 800-53 Rev. 5, profilo CRI v2.2	BASSO	✗ No	Periodic (Periodico)
PCA.1	AWS Private CA l'autorità di certificazione principale deve essere disabilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	BASSO	✗ No	Periodic (Periodico)
PCA.2	AWS Le autorità di certificazione CA private devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	✓ Sì	Modifica attivata
RDS.1	L'istantanea RDS deve essere privata	AWS Best practice di sicurezza di base v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, profilo CRI v2.2	CRITICO	✗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.2	Le istanze DB RDS devono vietare l'accesso pubblico, come stabilito dalla configurazione PubliclyAccessible	Benchmark CIS AWS Foundations v5.0.0, CIS Foundations Benchmark v3.0.0, migliori pratiche di sicurezza di base, NIST SP 800-53 Rev. 5 AWS , PCI DSS v3.2.1, PCI DSS v4.0.1, profilo AWS CRI v2.2	CRITICO	⊗ No	Modifica attivata
RDS.3	Le istanze DB RDS devono avere la crittografia a riposo abilitata	Benchmark CIS AWS Foundations v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Buone pratiche di sicurezza di base v1.0.0, AWS NIST SP 800-53 Rev. 5, profilo CRI v2.2 AWS	MEDIO	⊗ No	Modifica attivata
RDS.4	Le istantanee del cluster RDS e le istantanee del database devono essere crittografate quando sono inattive	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.5	Le istanze DB RDS devono essere configurate con più zone di disponibilità	Benchmark CIS AWS Foundations v5.0.0, migliori pratiche di sicurezza di AWS base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata
RDS.6	Il monitoraggio avanzato deve essere configurato per le istanze DB RDS	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	⊙ Sì	Modifica attivata
RDS.7	I cluster RDS devono avere la protezione da eliminazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata
RDS.8	Le istanze DB RDS devono avere la protezione da eliminazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	BASSO	⊗ No	Modifica attivata
RDS.9	Le istanze DB RDS devono pubblicare i log in Logs CloudWatch	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.10	L'autenticazione IAM deve essere configurata per le istanze RDS	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata
RDS.11	Le istanze RDS devono avere i backup automatici abilitati	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	Sì	Modifica attivata
RDS.12	L'autenticazione IAM deve essere configurata per i cluster RDS	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata
RDS.13	Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati	Benchmark CIS AWS Foundations v5.0.0, CIS Foundations Benchmark v3.0.0, migliori pratiche di sicurezza di base, NIST SP 800-53 Rev. 5 AWS , PCI DSS v4.0.1, AWS CRI Profile v2.2	HIGH (ELEVATO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.14	I cluster Amazon Aurora dovrebbero avere il backtracking abilitato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	Sì	Modifica attivata
RDS.15	I cluster RDS DB devono essere configurati per più zone di disponibilità	Benchmark CIS AWS Foundations v5.0.0, migliori pratiche di sicurezza di AWS base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	No	Modifica attivata
RDS.16	I cluster Aurora DB devono essere configurati per copiare i tag nelle istantanee DB	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	No	Modifica attivata
RDS.17	Le istanze DB RDS devono essere configurate per copiare i tag nelle istantanee	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.19	Gli abbonamenti esistenti per la notifica degli eventi RDS devono essere configurati per gli eventi critici del cluster	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata
RDS.20	Gli abbonamenti esistenti per la notifica degli eventi RDS devono essere configurati per gli eventi critici delle istanze di database	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata
RDS.21	È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.22	È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata
RDS.23	Le istanze RDS non devono utilizzare una porta predefinita del motore di database	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata
RDS.24	I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
RDS.25	Le istanze del database RDS devono utilizzare un nome utente di amministratore personalizzato	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
RDS.26	Le istanze DB RDS devono essere protette da un piano di backup	NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	✓ Sì	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.27	I cluster RDS DB devono essere crittografati quando sono inattivi	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata
RDS.28	I cluster RDS DB devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
RDS.29	Le istantanee del cluster RDS DB devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
RDS.30	Le istanze DB RDS devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
RDS.31	I gruppi di sicurezza RDS DB devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
RDS.32	Le istantanee RDS DB devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
RDS.33	I gruppi di sottoreti RDS DB devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.34	I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
RDS.35	Nei cluster RDS DB dovrebbe essere abilitato l'aggiornamento automatico delle versioni secondarie	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
RDS.36	Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	✓ Sì	Modifica attivata
RDS.37	I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
RDS.38	Le istanze DB RDS per PostgreSQL devono essere crittografate in transito	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.39	Le istanze DB RDS per MySQL devono essere crittografate in transito	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
RDS.40	Le istanze DB di RDS per SQL Server devono pubblicare i log in Logs CloudWatch	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sì	Modifica attivata
RDS.41	Le istanze DB di RDS per SQL Server devono essere crittografate in transito	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
RDS.42	Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch	AWS Migliori pratiche di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sì	Periodic (Periodico)
RDS.43	I proxy RDS DB devono richiedere la crittografia TLS per le connessioni	AWS Migliori pratiche di sicurezza di base	MEDIO	⊗ No	Periodic (Periodico)
RDS.44	Le istanze RDS per MariaDB DB devono essere crittografate in transito	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.45	I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
RDS.46	Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso gateway Internet	AWS Le migliori pratiche di sicurezza di base	HIGH (ELEVATO	⊗ No	Periodic (Periodico)
RDS.47	I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB.	AWS Le migliori pratiche di sicurezza di base	BASSO	⊗ No	Modifica attivata
RDS.48	I cluster DB RDS per MySQL devono essere configurati per copiare i tag nelle istantanee del DB	AWS Le migliori pratiche di sicurezza di base	BASSO	⊗ No	Modifica attivata
RDS.50	È necessario impostare un periodo di conservazione dei backup sufficiente per i cluster RDS DB	AWS Best practice di sicurezza di base v1.0.0	MEDIO	⊗ Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.51	I cluster globali RDS devono essere eseguiti su una versione di Aurora MySQL supportata	AWS Best practice di sicurezza di base	HIGH (ELEVATO	No	Modifica attivata
Redshift.1	I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	CRITICO	No	Modifica attivata
Redshift.2	Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Modifica attivata
Redshift.3	I cluster Amazon Redshift devono avere le istantanee automatiche abilitate	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	Sì	Modifica attivata
Redshift.4	I cluster Amazon Redshift devono avere la registrazione di controllo abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Redshift.6	Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
Redshift.7	I cluster Redshift devono utilizzare un routing VPC avanzato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
Redshift.8	I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
Redshift.10	I cluster Redshift devono essere crittografati quando sono inattivi	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
Redshift.11	I cluster Redshift devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata
Redshift.12	Le notifiche di sottoscrizione agli eventi Redshift devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Redshift.13	Le istantanee del cluster Redshift devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Redshift.14	I gruppi di sottoreti del cluster Redshift devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Redshift.15	I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
Redshift.16	I gruppi di sottoreti del cluster Redshift devono avere sottoreti provenienti da più zone di disponibilità	NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	No	Modifica attivata
Redshift.17	I gruppi di parametri del cluster Redshift devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Redshift.18	I cluster Redshift devono avere implementazioni abilitate Multi-AZ	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RedshiftServerless.1	I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato	AWS Best practice di sicurezza di base, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Periodic (Periodico)
RedshiftServerless.2	Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)
RedshiftServerless.3	I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico	AWS Best practice di sicurezza di base, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Periodic (Periodico)
RedshiftServerless.4	I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys	NIST SP 800-53 Rev. 5	MEDIO	⊙ Sì	Periodic (Periodico)
RedshiftServerless.5	I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito	AWS Best practice di sicurezza di base	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RedshiftServerless.6	I namespace Redshift Serverless devono esportare i log in Logs CloudWatch	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)
Route53.1	I controlli sanitari della Route 53 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Route53.2	Le zone ospitate pubbliche di Route 53 devono registrare le query DNS	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Modifica attivata
S3.1	I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate	Benchmark CIS AWS Foundations v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, migliori pratiche di sicurezza di base, NIST SP AWS 800-53 Rev. 5, PCI DSS v3.2.1 AWS , PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
S3.2	I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico alla lettura	AWS Best practice di sicurezza di base, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI Profile v2.2	CRITICO	⊗ No	Modifica attivata e periodica
S3.3	I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura	AWS Best practice di sicurezza di base, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI Profile v2.2	CRITICO	⊗ No	Modifica attivata e periodica
S3.5	I bucket S3 per uso generico dovrebbero richiedere l'utilizzo di SSL	Benchmark CIS AWS Foundations v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, migliori pratiche di sicurezza di base, NIST SP AWS 800-53 Rev. 5, NIST SP 800-171 Rev. 2 AWS , PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
S3.6	Le policy relative ai bucket per uso generico di S3 dovrebbero limitare l'accesso ad altri Account AWS	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Modifica attivata
S3.7	I bucket S3 per uso generico devono utilizzare la replica tra regioni	PCI DSS versione 3.2.1, NIST SP 800-53 Rev. 5, profilo CRI versione 2.2	BASSO	⊗ No	Modifica attivata
S3.8	I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Best practice di sicurezza di base, NIST SP 800-53 AWS Rev. 5, PCI DSS v4.0.1 AWS , CRI Profile v2.2	HIGH (ELEVATO	⊗ No	Modifica attivata
S3.9	I bucket S3 per uso generico devono avere la registrazione degli accessi al server abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
S3.10	I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita	NIST SP 800-53 Rev. 5, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata
S3.11	I bucket S3 per uso generico devono avere le notifiche degli eventi abilitate	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, profilo CRI v2.2	MEDIO	⊙ Sì	Modifica attivata
S3.12	Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
S3.13	I bucket S3 per uso generico devono avere configurazioni del ciclo di vita	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	BASSO	⊙ Sì	Modifica attivata
S3.14	I bucket S3 per uso generico devono avere il controllo delle versioni abilitato	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, profilo CRI v2.2	BASSO	⊗ No	Modifica attivata
S3.15	I bucket S3 per uso generico devono avere Object Lock abilitato	NIST SP 800-53 Rev. 5, PCI DSS versione 4.0.1, profilo CRI versione 2.2	MEDIO	⊙ Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
S3.17	I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS versione 4.0.1, profilo CRI v2.2	MEDIO	⊗ No	Modifica attivata
S3.19	I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	CRITICO	⊗ No	Modifica attivata
S3.20	I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, benchmark CIS AWS Foundations v1.4.0, NIST SP 800-53 Rev. 5, profilo CRI AWS v2.2	BASSO	⊗ No	Modifica attivata
S3.22	I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, PCI DSS AWS v4.0.1, profilo CRI v2.2	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
S3.23	I bucket S3 per uso generico dovrebbero registrare gli eventi di lettura a livello di oggetto	Benchmark CIS AWS Foundations v5.0.0, benchmark CIS Foundations v3.0.0, PCI DSS AWS v4.0.1, profilo CRI v2.2	MEDIO	No	Periodic (Periodico)
S3.24	I punti di Multi-Region accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate	AWS Best practice di sicurezza di base, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Modifica attivata
S3.25	I bucket di directory S3 devono avere configurazioni del ciclo di vita	AWS Best practice di sicurezza di base	BASSO	Sì	Modifica attivata
SageMaker.1	Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	HIGH (ELEVATO	No	Periodic (Periodico)
SageMaker.2	SageMaker le istanze dei notebook devono essere avviate in un VPC personalizzato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	HIGH (ELEVATO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SageMaker.3	Gli utenti non devono avere accesso root alle istanze del SageMaker notebook	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	HIGH (ELEVATO)	No	Modifica attivata
SageMaker.4	SageMaker le varianti di produzione endpoint devono avere un numero iniziale di istanze superiore a 1	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)
SageMaker.5	SageMaker i modelli devono avere l'isolamento della rete abilitato	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	No	Modifica attivata
SageMaker.6	SageMaker le configurazioni delle immagini delle app devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
SageMaker.7	SageMaker le immagini devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
SageMaker.8	SageMaker le istanze di notebook devono essere eseguite su piattaforme supportate	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SageMaker.9	SageMaker le definizioni dei lavori relativi alla qualità dei dati dovrebbero avere la crittografia del traffico tra container abilitata	AWS Best practice di sicurezza di base v1.0.0	MEDIO	⊗ No	Modifica attivata
SageMaker.10	SageMaker le definizioni dei processi di spiegabilità dei modelli devono avere abilitata la crittografia del traffico tra container	AWS Best practice di sicurezza di base v1.0.0	MEDIO	⊗ No	Modifica attivata
SageMaker.11	SageMaker le definizioni dei processi di qualità dei dati devono avere l'isolamento della rete abilitato	AWS Best practice di sicurezza di base v1.0.0	MEDIO	⊗ No	Modifica attivata
SageMaker.12	SageMaker le definizioni dei job di model bias dovrebbero avere l'isolamento della rete abilitato	AWS Best practice di sicurezza di base v1.0.0	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SageMaker.13	SageMaker le definizioni dei processi di qualità del modello dovrebbero avere la crittografia del traffico tra container abilitata	AWS Best practice di sicurezza di base v1.0.0	MEDIO	⊗ No	Modifica attivata
SageMaker.14	SageMaker le pianificazioni di monitoraggio dovrebbero avere l'isolamento della rete abilitato	AWS Best practice di sicurezza di base v1.0.0	MEDIO	⊗ No	Modifica attivata
SageMaker.15	SageMaker le definizioni dei job di model bias devono avere abilitata la crittografia del traffico tra container	AWS Best practice di sicurezza di base v1.0.0	MEDIO	⊗ No	Modifica attivata
SageMaker.16	SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari	AWS Le migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SageMaker.17	SageMaker i negozi offline dei gruppi di funzionalità devono essere crittografati con chiavi AWS KMS	AWS Le migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata
SageMaker.18	SageMaker i negozi online di gruppi di funzionalità con archiviazione standard devono essere crittografati con chiavi AWS KMS	NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Modifica attivata
SageMaker.19	SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore	AWS Le migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata
SageMaker.20	SageMaker le definizioni dei processi di spiegabilità del modello dovrebbero avere l'isolamento della rete abilitato	AWS Le migliori pratiche di sicurezza di base	HIGH (ELEVATO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SageMaker.21	SageMaker le istanze dei notebook devono essere crittografate con chiavi gestite dal cliente AWS KMS	AWS Best practice di sicurezza di base	MEDIO	⊗ No	Modifica attivata
SageMaker.22	SageMaker le pianificazioni di monitoraggio dovrebbero avere la crittografia del traffico tra container abilitata	AWS Le migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata
SageMaker.23	SageMaker gli esperimenti di inferenza dovrebbero avere il volume di archiviazione delle istanze crittografato con chiavi gestite dal cliente AWS KMS	AWS Le migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata
SageMaker.24	SageMaker gli esperimenti di inferenza dovrebbero avere l'archiviazione dei dati crittografata con chiavi gestite dal cliente AWS KMS	AWS Le migliori pratiche di sicurezza di base	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SageMaker.25	SageMaker le definizioni dei processi di qualità del modello dovrebbero avere l'isolamento della rete abilitato	AWS Migliori pratiche di sicurezza di base	HIGH (ELEVATO	⊗ No	Modifica attivata
SecretsManager.1	I segreti di Secrets Manager devono avere la rotazione automatica abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊙ Sì	Modifica attivata
SecretsManager.2	I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
SecretsManager.3	Rimuovi i segreti inutilizzati di Secrets Manager	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊙ Sì	Periodic (Periodico)
SecretsManager.4	I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	⊙ Sì	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SecretsManager.5	I segreti di Secrets Manager devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
ServiceCatalog.1	I portafogli Service Catalog devono essere condivisi solo all'interno di un' AWS organizzazione.	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)
SES.1	Gli elenchi di contatti SES devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
SES.2	I set di configurazione SES devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
SES.3	I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail	AWS Migliori pratiche di sicurezza di base	MEDIO	No	Modifica attivata
SNS.1	Gli argomenti SNS devono essere crittografati a riposo utilizzando AWS KMS	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, profilo CRI v2.2	MEDIO	No	Modifica attivata
SNS.3	Gli argomenti SNS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SNS.4	Le politiche di accesso agli argomenti di SNS non dovrebbero consentire l'accesso pubblico	AWS Best practice di sicurezza di base, CRI Profile v2.2	CRITICO	⊗ No	Modifica attivata
SQS.1	Le code Amazon SQS devono essere crittografate quando sono inattive	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
SQS.2	Le code SQS devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	⊙ Sì	Modifica attivata
SQS.3	Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico	AWS Best practice di sicurezza di base, CRI Profile v2.2	CRITICO	⊗ No	Modifica attivata
SSM.1	Le istanze EC2 devono essere gestite da AWS Systems Manager	AWS Best practice di sicurezza di base v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SSM.2	Le istanze EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch.	AWS Best practice di sicurezza di base 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 (ELEVATO	⊗ No	Modifica attivata
SSM.3	Le istanze EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, CRI Profile v2.2	BASSO	⊗ No	Modifica attivata
SSM.4	I documenti SSM non devono essere pubblici	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, profilo CRI v2.2	CRITICO	⊗ No	Periodic (Periodico)
SSM.5	I documenti SSM devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	✓ Sì	Modifica attivata
SSM.6	SSM Automation dovrebbe avere CloudWatch la registrazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, CRI Profile v2.2	MEDIO	⊗ No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SSM.7	I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, CRI Profile v2.2	CRITICO	No	Periodic (Periodico)
StepFunctions.1	Le macchine a stati Step Functions dovrebbero avere la registrazione attivata	AWS Buone pratiche di sicurezza di base v1.0.0, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	Sì	Modifica attivata
StepFunctions.2	Le attività di Step Functions devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Transfer.1	I flussi di lavoro Transfer Family devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Transfer.2	I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)
Transfer.3	I connettori Transfer Family devono avere la registrazione abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Transfer.4	Gli accordi Transfer Family devono essere etichettati	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
Transfer.5	I certificati Transfer Family devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Transfer.6	I connettori Transfer Family devono essere etichettati	AWS Resource Tagging Standard, CRI Profile v2.2	BASSO	Sì	Modifica attivata
Transfer.7	I profili Transfer Family devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
WAF.1	AWS La registrazione WAF Classic Global Web ACL deve essere abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, CRI Profile v2.2	MEDIO	No	Periodic (Periodico)
WAF.2	AWS Le regole regionali di WAF Classic devono avere almeno una condizione	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata
WAF.3	AWS I gruppi di regole regionali WAF Classic devono avere almeno una regola	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
WAF.4	AWS Gli ACL web regionali di WAF Classic devono avere almeno una regola o un gruppo di regole	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
WAF.6	AWS Le regole globali di WAF Classic devono avere almeno una condizione	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
WAF.7	AWS I gruppi di regole globali di WAF Classic devono avere almeno una regola	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
WAF.8	AWS Gli ACL web globali di WAF Classic devono avere almeno una regola o un gruppo di regole	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
WAF.10	AWS Gli ACL Web WAF devono avere almeno una regola o un gruppo di regole	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
WAF.11	AWS La registrazione ACL Web WAF deve essere abilitata	NIST SP 800-53 Rev. 5, PCI DSS versione 4.0.1, profilo CRI versione 2.2	BASSO	⊗ No	Periodic (Periodico)
WAF.12	AWS Le regole WAF devono avere le CloudWatch metriche abilitate	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
WorkSpaces.1	WorkSpaces i volumi utente devono essere crittografati quando sono inattivi	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata
WorkSpaces.2	WorkSpaces i volumi root devono essere crittografati quando sono inattivi	AWS Best practice di sicurezza di base, CRI Profile v2.2	MEDIO	⊗ No	Modifica attivata

Registro delle modifiche per i controlli CSPM di Security Hub

Il seguente registro delle modifiche tiene traccia delle modifiche sostanziali ai controlli CSPM esistenti di AWS Security Hub, che possono comportare modifiche allo stato generale di un controllo e allo stato di conformità dei risultati. Per informazioni su come Security Hub CSPM valuta lo stato del controllo, vedere. Valutazione dello stato di conformità e dello stato di controllo Le modifiche possono richiedere alcuni giorni dopo la loro immissione in questo registro per avere effetto su tutte le aree Regioni AWS in cui il controllo è disponibile.

Questo registro tiene traccia delle modifiche avvenute dall'aprile 2023. Scegli un controllo per visualizzare ulteriori dettagli al riguardo. Le modifiche al titolo vengono annotate nella descrizione dettagliata di un controllo per 90 giorni.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 ottobre 2026	[Bedrock.1] Le fonti di dati Amazon Bedrock devono essere crittografate e gestite dai clienti AWS KMS keys	Security Hub CSPM ha aggiornato il controllo per non valutare le fonti di dati che apparteng ono a una knowledge base gestita, poiché la crittografia lato server per una knowledge base gestita è configurata sulla knowledge base anziché sulle relative fonti di dati.
23 settembre 2026	[BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC	Security Hub CSPM ha aggiornato il controllo per non valutare i runtime supportati da un provider di capacità, poiché tali runtime definiscono la configurazione di rete sul provider di capacità anziché sul runtime.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
11 settembre 2026	[] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato	Questo controllo verifica se l'aggiorn amento automatic o della versione secondaria è abilitato per un cluster Amazon RDS DB. Security Hub CSPM ha esteso il controllo per valutare i cluster Aurora DB, che in precedenza non restituivano risultati.
11 settembre 2026	[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS	Security Hub CSPM ha aggiornato il titolo e la descrizione di questo controllo per fare riferimento a TLS anziché a SSL poiché SSL è obsoleto.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
27 agosto 2026	[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible	Questo controllo verifica se le istanze Amazon RDS vietano l'accesso pubblico. Poiché Neptune DB ora supporta gli endpoint pubblici, questo controllo valuta e genera risultati utilizzabili per le istanze di Neptune DB. Security Hub CSPM ha aggiornato la descrizione del controllo per riflettere questa modifica.
12 agosto 2026	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Questo controllo verifica se un cluster Amazon EKS viene eseguito su una versione Kubernetes supportata. Security Hub CSPM ha modificato il valore del parametro per questo controllo da `a1.33. 1.34` Il supporto standard per Kubernetes versione 1.33 in Amazon EKS è terminato il 29 luglio 2026.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 agosto 2026	[EKS.9] I gruppi di nodi EKS devono essere eseguiti su una versione di Kubernetes supportata	Questo controllo verifica se un gruppo di nodi Amazon EKS funziona su una versione Kubernetes supportata. Security Hub CSPM ha modificato il valore del parametro per questo controllo da a`1.33`. `1.34` Il supporto standard per Kubernetes versione 1.33 in Amazon EKS è terminato il 29 luglio 2026.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
3 agosto 2026	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `java17.al2023`, `java11.al2023`, `java8.al2023` come valore di parametro, così come AWS Lambda è stato aggiunto il supporto per questo runtime.
3 agosto 2026	[EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio	Security Hub CSPM ha rimosso questo controllo dallo standard AWS Foundational Security Best Practices (FSBP).

Data di modifica	ID e titolo del controllo	Descrizione della modifica
31 luglio 2026	[SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate	Security Hub CSPM ha modificato il valore del parametro per questo controllo da `anotebook-al2-v3`. `notebook-al2023-v1` SageMaker L'intelligenza artificiale ha migrato le piattaforme di istanze di notebook da Amazon Linux 2 a AL2023.
13 luglio 2026	[EC2.10] Amazon EC2 deve essere configurato per utilizzare gli endpoint VPC creati per il servizio Amazon EC2	Security Hub CSPM ha modificato la regola di supporto per questo controllo da service-vpc-endpoint-enabled a vpc-endpoint-enabled. La regola aggiornata riconosce i nomi dei servizi degli endpoint come conformi e genera un risultato per i VPC che utilizzano endpoint FIPS. FIPS-variant `PASSED`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
29 giugno 2026	[EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio	Security Hub CSPM ha aggiunto questo controllo ai seguenti standard applicabili: lo standard NIST SP 800-53 Rev. 5, lo standardNIST SP 800-171 Revision 2 e lo standard PCI DSS v4.0.1. Il 30 luglio 2026, questo controllo verrà rimosso dallo standard Foundational Security Best Practices (FSBP).AWS
5 giugno 2026	[EKS.3] I cluster EKS devono utilizzare segreti Kubernetes crittografati	Security Hub CSPM ha comunicato che questo controllo verrà ritirato e rimosso da tutti gli standard CSPM di Security Hub applicabili dopo il 10 agosto 2026. A partire dalla versione 1.28 di Kubernetes, i cluster Amazon EKS dispongono di segreti Kubernetes protetti con crittografia a busta per impostazione predefinita.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 giugno 2026	[IoTEvents.1] Gli input di AWS IoT Events devono essere etichettati	Security Hub CSPM ha comunicato che questo controllo verrà ritirato e rimosso da tutti gli standard CSPM di Security Hub applicabili dopo il 7 luglio 2026. AWS ha annunciato la fine del supporto per il servizio AWS IoT Events a partire dal 20 maggio 2026.
5 giugno 2026	[IoTEvents.2] I modelli di rilevatori AWS IoT Events devono essere etichettati	Security Hub CSPM ha comunicato che questo controllo verrà ritirato e rimosso da tutti gli standard CSPM di Security Hub applicabili dopo il 7 luglio 2026. AWS ha annunciato la fine del supporto per il servizio AWS IoT Events a partire dal 20 maggio 2026.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 giugno 2026	[IoTEvents.3] I modelli di allarme AWS IoT Events devono essere etichettati	Security Hub CSPM ha comunicato che questo controllo verrà ritirato e rimosso da tutti gli standard CSPM di Security Hub applicabili dopo il 7 luglio 2026. AWS ha annunciato la fine del supporto per il servizio AWS IoT Events a partire dal 20 maggio 2026.
5 giugno 2026	[ECS.1] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard applicabili. In precedenza, il controllo verificava se una definizione di attività Amazon ECS attiva che utilizzava la modalità di rete host `privileged` disponesse anche di definizioni di `user` container.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 giugno 2026	[RDS.18] Le istanze RDS devono essere distribuite in un VPC	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard applicabili. Da quando la EC2-Classic rete Amazon è stata ritirata, le istanze di Amazon Relational Database Service (Amazon RDS) non possono più essere distribui te al di fuori di un VPC. In precedenza, il controllo verificava se un'istanza Amazon RDS fosse stata distribuita su un. EC2-VPC

Data di modifica	ID e titolo del controllo	Descrizione della modifica
4 maggio 2026	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `ruby4.0` come parametro e non include più questo `nodejs20.x` runtime come AWS Lambda obsoleto.
27 aprile 2026	[EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato	Security Hub CSPM ha cambiato la regola di supporto per questo controllo da ec2-stopped-instance a una regola CSPM Security Hub personalizzata, ec2-stopped-instance-days-check per semplificare la logica di valutazione.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
7 aprile 2026	[EC2.1] Le istantanee di Amazon EBS non devono essere configurate per essere ripristinabili pubblicamente	Security Hub CSPM ha modificato il titolo e la descrizione di questo controllo. Il nuovo titolo e la nuova descrizione riflettono in modo più accurato che il controllo verifica se gli snapshot di Amazon EBS sono configurati per essere ripristinabili pubblicamente. In precedenza, il titolo di questo controllo era: gli snapshot di Amazon EBS non dovrebbero essere ripristinabili pubblicamente.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
7 aprile 2026	[EC2.182] Le impostazioni di blocco dell'accesso pubblico devono essere abilitate per gli snapshot di Amazon EBS	Security Hub CSPM ha modificato il titolo e la descrizione di questo controllo. Il nuovo titolo e la nuova descrizione riflettono in modo più accurato che il controllo verifica se l'accesso pubblico a blocchi a livello di account è abilitato per gli snapshot di Amazon EBS. In precedenza, il titolo di questo controllo era: Amazon EBS Snapshots non dovrebbe essere accessibile al pubblico.
6 aprile 2026	[ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate	Security Hub CSPM ha aggiornato il valore del parametro per questo controllo in modo che rifletta le politiche di sicurezza consigliate.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
3 aprile 2026	[Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate	Security Hub CSPM ha ampliato la gamma di valori supportati per il `temporaryPasswordValidity` parametro di questo controllo. Ora puoi specificare un valore compreso tra 1 e 365 giorni. In precedenza, l'intervallo era di 7-365 giorni.
3 aprile 2026	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Questo controllo verifica se un cluster Amazon EKS viene eseguito su una versione Kubernetes supportata. Security Hub CSPM ha modificato il valore del parametro per questo controllo da `a1.32`. `1.33` Il supporto standard per Kubernetes versione 1.32 in Amazon EKS è terminato il 23 marzo 2026.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
3 aprile 2026	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 il parametro per i runtime supportat i non è più incluso `ruby3.2` poiché Lambda ha reso obsoleto questo runtime.
24 marzo 2026	[RDS.50] I cluster RDS DB devono avere un periodo di conservazione dei backup sufficiente	Security Hub CSPM ha aggiornato il titolo del controllo per indicare che il controllo controlla tutti i cluster DB RDS.
24 marzo 2026	[ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root	Security Hub CSPM ha aggiornato il titolo e la descrizione del controllo per indicare che il controllo verifica le definizioni delle attività ECS. Security Hub CSPM ha inoltre aggiornato il controllo per non generare risultati per le definizio ni delle attività con `runtimePl atform` configura to per specifica re una famiglia di `WINDOWS_SERVER` sistemi operativi.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
9 marzo 2026	[AppSync.1] Le cache AWS AppSync delle API devono essere crittografate quando sono inattive	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso dallo standard AWS Foundational Security Best Practices (FSBP). AWS AppSync ora fornisce la crittografia predefinita su tutte le cache API attuali e future.
9 marzo 2026	[AppSync.6] Le cache AWS AppSync delle API devono essere crittografate in transito	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso dallo standard AWS Foundational Security Best Practices (FSBP). AWS AppSync ora fornisce la crittografia predefinita su tutte le cache API attuali e future.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
4 marzo 2026	[ECS.1] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso dallo standard AWS Foundational Security Best Practices (FSBP) e dallo standard NIST SP 800-53 Rev. 5.
5 febbraio 2026	[AppSync.1] Le cache AWS AppSync delle API devono essere crittografate quando sono inattive	Security Hub CSPM ritirerà questo controllo e lo rimuoverà da tutti gli standard CSPM di Security Hub applicabili il 9 marzo 2026. AWS AppSync fornisce la crittografia predefinita su tutte le cache API attuali e future.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 febbraio 2026	[AppSync.6] Le cache AWS AppSync delle API devono essere crittografate in transito	Security Hub CSPM ritirerà questo controllo e lo rimuoverà da tutti gli standard CSPM di Security Hub applicabili il 9 marzo 2026. AWS AppSync fornisce la crittografia predefinita su tutte le cache API attuali e future.
16 gennaio 2026	[ECS.1] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure	Security Hub CSPM ha comunicato che questo controllo verrà ritirato e rimosso da tutti gli standard CSPM di Security Hub applicabili dopo il 16 febbraio 2026.
12 gennaio 2026	[Redshift.4] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata	Security Hub CSPM ha aggiornato questo controllo per rimuovere il `loggingEnabled` parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 gennaio 2026	[MQ.3] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie	Security Hub CSPM ha ritirato il controllo e lo ha rimosso da tutti gli standard applicabili. Security Hub CSPM ha ritirato il controllo a causa dei requisiti di Amazon MQ per gli aggiornamenti automatici delle versioni secondarie. In precedenza, il controllo si applicava allo standard AWS Foundational Security Best Practices (FSBP), allo standardNIST SP 800-53 Rev. 5 e allo standard PCI DSS v4.0.1.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 gennaio 2026	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Questo controllo verifica se le impostazioni di runtime per una AWS Lambda funzione corrispondono ai valori previsti per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `dotnet10` come valore di parametro per questo controllo. AWS Lambda ha aggiunto il supporto per questo runtime.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
15 dicembre 2025	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Questo controllo verifica se le impostazioni di runtime per una AWS Lambda funzione corrispondono ai valori previsti per i runtime supportat i in ogni lingua. Security Hub CSPM non supporta più `python3.9` come valore di parametro per questo controllo . AWS Lambda non supporta più questo runtime.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 dicembre 2025	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Questo controllo verifica se un cluster Amazon EKS viene eseguito su una versione Kubernetes supportata. Security Hub CSPM ha modificato il valore del parametro per questo controllo da `a1.31. 1.32` Il supporto standard per Kubernetes versione 1.31 in Amazon EKS è terminato il 26 novembre 2025.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
21 novembre 2025	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Questo controllo verifica se le impostazioni di runtime per una AWS Lambda funzione corrispondono ai valori previsti per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `nodejs24.x` e `python3.14` come valori dei parametri per questo controllo. AWS Lambda ha aggiunto il supporto per questi runtime.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 novembre 2025	[EC2.15] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici	Security Hub CSPM ha aggiornato la descrizione e le motivazioni di questo controllo. In precedenza, il controllo controllava solo l'assegnazione automatica degli IP pubblici IPv4 nelle sottoreti Amazon VPC utilizzando il flag. `MapPublicIpOnLaunch` Questo controllo ora verifica l'assegnazione automatica degli IP pubblici sia a IPv4 che a IPv6. La descrizione e la motivazione del controllo sono state aggiornate per riflettere queste modifiche.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 novembre 2025	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Questo controllo verifica se le impostazioni di runtime per una AWS Lambda funzione corrispondono ai valori previsti per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `java25` come valore di parametro per questo controllo. AWS Lambda ha aggiunto il supporto per questo runtime.
13 novembre 2025	[SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico	Security Hub CSPM ha modificato la gravità di questo controllo da a`HIGH`. `CRITICAL` Consentire l'accesso pubblico agli argomenti di Amazon SNS rappresenta un rischio significativo per la sicurezza.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
13 novembre 2025	[SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico	Security Hub CSPM ha modificato la gravità di questo controllo da a`HIGH`. `CRITICAL` Consentire l'accesso pubblico alle code di Amazon SQS rappresenta un rischio significativo per la sicurezza.
13 novembre 2025	[GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato	Security Hub CSPM ha modificato la gravità di questo controllo da a`MEDIUM`. `HIGH` Questo tipo di monitoraggio del runtime fornisce un rilevamento avanzato delle minacce per le risorse Amazon EKS.
13 novembre 2025	[MQ.3] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie	Security Hub CSPM ha modificato la gravità di questo controllo da a`LOW`. `MEDIUM` Gli aggiornamenti di versione minori includono le patch di sicurezza necessarie per mantenere la sicurezza del broker Amazon MQ.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
13 novembre 2025	[Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software	Security Hub CSPM ha modificato la gravità di questo controllo da `LOW`. `MEDIUM` Gli aggiornamenti software includono patch di sicurezza necessari e per mantenere OpenSearch la sicurezza del dominio.
13 novembre 2025	[RDS.7] I cluster RDS devono avere la protezione da eliminazione abilitata	Security Hub CSPM ha modificato la gravità di questo controllo da `LOW`. `MEDIUM` La protezione dall'eliminazione aiuta a prevenire l'eliminazione accidentale dei database Amazon RDS e l'eliminazione dei database RDS da parte di entità non autorizzate.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
13 novembre 2025	[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs	Security Hub CSPM ha modificato la gravità di questo controllo da a`LOW`. `MEDIUM` AWS CloudTrail i dati di registrazione in Amazon CloudWatch Logs possono essere utilizzati per attività di audit, allarmi e altre importanti operazioni di sicurezza.
13 novembre 2025	[ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione	Security Hub CSPM ha modificato la gravità di questo controllo da a`HIGH`. `MEDIUM` La condivisi one di AWS Service Catalog portafogl i con account specifici potrebbe essere intenzion ale e non indica necessariamente che un portafoglio sia accessibile al pubblico.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
13 novembre 2025	[CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS	Security Hub CSPM ha modificato la gravità di questo controllo da a`MEDIUM`. `LOW` I nomi di `cloudfront.net` dominio predefiniti per CloudFront le distribuzioni Amazon vengono generati in modo casuale, il che riduce i rischi per la sicurezza.
13 novembre 2025	[ELB.7] I Classic Load Balancer dovrebbero avere abilitato il drenaggio della connessione	Security Hub CSPM ha modificato la gravità di questo controllo da a`MEDIUM`. `LOW` Nelle implement azioni a più istanze, altre istanze integre possono gestire le sessioni utente quando un'istanza viene terminata senza esaurire la connessio ne, il che riduce l'impatto operativo e i rischi di disponibilità.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
13 novembre 2025	[RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito	Security Hub CSPM ha aggiornato questo controllo per rimuovere il parametro opzionale `validAdminUserNames` .
23 ottobre 2025	I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati	Security Hub CSPM ha annullato le modifiche apportate al titolo, alla descrizione e alla regola per questo controllo il 14 ottobre 2025.
22 ottobre 2025	[CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato	Security Hub CSPM ha aggiornato questo controllo per non generare risultati per le CloudFront distribuzioni Amazon che utilizzano origini personalizzate.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 ottobre 2025	[CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata	Questo controllo verifica se una CloudFront distribuzione Amazon è configurata per utilizzare una politica di sicurezza TLS consigliata. Security Hub CSPM ora supporta `TLSv1.2_2025` e `TLSv1.3_2025` come valori dei parametri per questo controllo.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 ottobre 2025	I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati	Security Hub CSPM ha modificato il titolo, la descrizione e la regola per questo controllo. In precedenza, il controllo controllava i cluster Redis OSS e tutti i gruppi di replica, utilizzando la regola elasticache-redis-cluster-automatic-backup-check. Il titolo del controllo era: (Redis OSS) i cluster dovrebbero avere i backup automatici abilitati. ElastiCache Questo controllo ora controlla i cluster Valkey oltre ai cluster Redis OSS e tutti i gruppi di replica, utilizzando la regola elasticache-automatic-backup-check-enabled. Il nuovo titolo e la nuova descrizione indicano che il controllo controlla entrambi i tipi di cluster.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 ottobre 2025	[Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software	La regola per questo controllo è stata aggiornata per generare anche un `PASSED` risultato se un dominio Amazon OpenSearch Service non ha aggiornamenti software disponibili e lo stato dell'aggiornamento non è idoneo. In precedenza, questo controllo generava un `PASSED` risultato solo se un OpenSearch dominio non aveva aggiornamenti software disponibili e lo stato dell'aggiornamento era completo.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
24 settembre 2025	[Redshift.9] I cluster Redshift non devono utilizzare il nome di database predefinito [RedshiftServerless.7] I namespace Redshift Serverless non devono utilizzare il nome di database predefinito	Security Hub CSPM ha ritirato questi controlli e li ha rimossi da tutti gli standard applicabili. Security Hub CSPM ha ritirato questi controlli a causa delle limitazioni intrinseche di Amazon Redshift che impedivano l'efficace correzione dei risultati dei controlli. `FAILED` In precedenza, i controlli si applicavano allo standard AWS Foundational Security Best Practices (FSBP) e allo standard NIST SP 800-53 Rev. 5. Il Redshift.9 controllo si applicava anche allo standard gestito dai servizi.AWS Control Tower

Data di modifica	ID e titolo del controllo	Descrizione della modifica
9 settembre 2025	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Questo controllo verifica se le impostazioni di runtime per una AWS Lambda funzione corrispondono ai valori previsti per i runtime supportat i in ogni lingua. Security Hub CSPM non supporta più `nodejs18.x` come valore di parametro per questo controllo . AWS Lambda non supporta più Node.js 18 runtime.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
13 agosto 2025	[SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato	Security Hub CSPM ha modificato il titolo e la descrizione di questo controllo. Il nuovo titolo e la nuova descrizione riflettono in modo più accurato che il controllo verifica l'impostazione del `EnableNetworkIsolation` parametro dei modelli ospitati da Amazon SageMaker AI. In precedenza, il titolo di questo controllo era: SageMaker models should block inbound traffic.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
13 agosto 2025	[EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio	Security Hub CSPM ha modificato il titolo e la descrizione di questo controllo. Il nuovo titolo e la nuova descrizione riflettono in modo più preciso l'ambito e la natura del controllo eseguito dal controllo. In precedenza, il titolo di questo controllo era: EFS mount targets should not be associated with a public subnet.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
24 luglio 2025	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Questo controllo verifica se un cluster Amazon EKS viene eseguito su una versione Kubernetes supportata. Security Hub CSPM ha modificato il valore del parametro per questo controllo da a`1.30`. `1.31` Il supporto standard per la versione 1.30 di Kubernetes in Amazon EKS è terminato il 23 luglio 2025.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
23 luglio 2025	[EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati	Security Hub CSPM ha cambiato il titolo di questo controllo. Il nuovo titolo riflette in modo più accurato che il controllo controlla solo le richieste Spot Fleet di Amazon EC2 che specificano i parametri di lancio. In precedenza, il titolo di questo controllo era: EC2 Spot Fleet requests should enable encryption for attached EBS volumes.
30 giugno 2025	[IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo	Security Hub CSPM ha rimosso questo controllo dallo standard PCI DSS v4.0.1. PCI DSS v4.0.1 non richiede esplicitamente l'uso di simboli nelle password.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
30 giugno 2025	[IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno	Security Hub CSPM ha rimosso questo controllo dallo standard NIST SP 800-171 Revision 2. NIST SP 800-171 Revisione 2 non richiede esplicita mente periodi di scadenza delle password di 90 giorni o meno.
30 giugno 2025	[RDS.16] I cluster Aurora DB devono essere configurati per copiare i tag nelle istantanee DB	Security Hub CSPM ha cambiato il titolo di questo controllo. Il nuovo titolo riflette in modo più accurato che il controllo controlla solo i cluster DB di Amazon Aurora. In precedenza, il titolo di questo controllo era:. RDS DB clusters should be configure d to copy tags to snapshots

Data di modifica	ID e titolo del controllo	Descrizione della modifica
30 giugno 2025	[SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate	Questo controllo verifica se un'istanza di notebook Amazon SageMaker AI è configurata per l'esecuzione su una piattaforma supportata, in base all'identificatore della piattaforma specificato per l'istanza del notebook. Security Hub CSPM non supporta più `notebook-al2-v1` e `notebook-al2-v2` come valori dei parametri per questo controllo. Le istanze di notebook eseguite su queste piattaforme hanno raggiunto la fine del supporto il 30 giugno 2025.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
30 maggio 2025	[IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide	Security Hub CSPM ha rimosso questo controllo dallo standard PCI DSS v4.0.1. Questo controllo verifica se le politiche relative alle password degli account per gli utenti IAM soddisfano i requisiti minimi, inclusa una lunghezza minima della password di 7 caratteri. PCI DSS v4.0.1 ora richiede che le password abbiano un minimo di 8 caratteri. Il controllo continua ad applicarsi allo standard PCI DSS v3.2.1, che ha requisiti di password diversi. Per valutare le politiche relative alle password degli account rispetto ai requisiti PCI DSS v4.0.1, puoi utilizzare il controllo. IAM.7 Questo controllo richiede che le

Data di modifica	ID e titolo del controllo	Descrizione della modifica
		password abbiano un minimo di 8 caratteri . Supporta anche valori personalizzati per la lunghezza della password e altri parametri. Il IAM.7 controllo fa parte dello standard PCI DSS v4.0.1 in Security Hub CSPM.
8 maggio 2025	[RDS.46] Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso i gateway Internet	Security Hub CSPM ha ripristinato completamente il rilascio del RDS.46 controllo. Regioni AWS In precedenz a, questo controllo supportava lo standard AWS Foundational Security Best Practices (FSBP).

Data di modifica	ID e titolo del controllo	Descrizione della modifica
7 aprile 2025	[ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate	Questo controllo verifica se il listener HTTPS per un Application Load Balancer o il listener TLS per un Network Load Balancer è configurato per crittografare i dati in transito utilizzando una politica di sicurezza consigliata. Security Hub CSPM ora supporta due valori di parametro aggiuntivi per questo controllo: `ELBSecurityPolicy-TLS13-1-2-Res-2021-06` e. `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
27 marzo 2025	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Questo controllo verifica se le impostazioni di runtime per una AWS Lambda funzione corrispondono ai valori previsti per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `ruby3.4` come valore di parametro per questo controllo. AWS Lambda ha aggiunto il supporto per questo runtime.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
26 marzo 2025	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Questo controllo verifica se un cluster Amazon Elastic Kubernetes Service (Amazon EKS) viene eseguito su una versione di Kubernetes supportata. Per il `oldestVersionSupported` parametro, Security Hub CSPM ha modificato il valore da a`1.29`. `1.30` La versione più vecchia di Kubernetes supportata è ora. `1.30`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 marzo 2025	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Questo controllo verifica se le impostazioni di runtime per una AWS Lambda fu nzione corrispon dono ai valori previsti per i runtime supportati in ogni lingua. Security Hub CSPM non supporta più `dotnet6` e `python3.8` come valori dei parametri per questo controllo . AWS Lambda non supporta più questi runtime.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
7 marzo 2025	[RDS.18] Le istanze RDS devono essere distribuite in un VPC	Security Hub CSPM ha rimosso questo controllo dallo standard AWS Foundational Security Best Practices e dai controlli automatici per i requisiti NIST SP 800-53 Rev. 5. Da quando la EC2-Class ic rete Amazon è stata ritirata, le istanze di Amazon Relationa l Database Service (Amazon RDS) non possono più essere distribuite al di fuori di un VPC.
10 gennaio 2025	[Glue.2] I lavori AWS Glue dovrebbero avere la registrazione abilitata	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard.
20 dicembre 2024	EC2.61 attraverso EC2.169	Security Hub CSPM ha ripristinato il rilascio dei controlli EC2.61 EC2.169 passanti.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 dicembre 2024	[RDS.23] Le istanze RDS non devono utilizzare una porta predefinita del motore di database	RDS.23 verifica se un cluster o un'istanza di Amazon Relational Database Service (Amazon RDS) utilizza una porta diversa dalla porta predefinita del motore di database. Abbiamo aggiornato il controllo in modo che la AWS Config regola sottostante restituisca un risultato di `NOT_APPLICABLE` per le istanze RDS che fanno parte di un cluster.
2 dicembre 2024	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `nodejs22.x` come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
26 novembre 2024	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Questo controllo verifica se un cluster Amazon Elastic Kubernetes Service (Amazon EKS) viene eseguito su una versione di Kubernetes supportata. La versione più vecchia supportata è ora `1.29`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
20 novembre 2024	[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse	Config.1 verifica se AWS Config è abilitato, utilizza il ruolo collegato al servizio e registra le risorse per i controlli abilitati. Security Hub CSPM ha aumentato la severità di questo controllo da a`MEDIUM`. `CRITICAL` Security Hub CSPM ha inoltre aggiunto nuovi codici di stato e motivi di stato per i risultati non riusciti Config.1 . Queste modifiche riflettono l'importanza dei controlli CSPM di Security Hub Config.1 per il funzionamento. Se hai AWS Config disabilitato la registrazione delle risorse, potresti ricevere risultati di controllo imprecisi. Per ricevere un `PASSED` risultato per Config.1, attiva la registrazione delle risorse per le risorse che corrispondono

Data di modifica	ID e titolo del controllo	Descrizione della modifica
		ai controlli CSPM di Security Hub abilitati e disabilita i controlli che non sono richiesti nella tua organizza zione. Per istruzioni sulla configurazione AWS Config per Security Hub CSPM, vedere. Attivazione e configurazione AWS Config per Security Hub CSPM Per un elenco dei controlli CSPM di Security Hub e delle relative risorse, vedere. Richiesto AWS Config risorse per i risultati del controllo
12 novembre 2024	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispon dono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `python3.13` come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
11 ottobre 2024	ElastiCache controlli	Titoli di controllo modificati per ElastiCache.3 ElastiCache.4, ElastiCache.5, e ElastiCache.7. I titoli non menzionano più Redis OSS perché i controlli si applicano anche a ElastiCache Valkey.
27 settembre 2024	[ELB.4] Application Load Balancer deve essere configurato per eliminare le intestazioni http non valide	Il titolo di controllo modificato da Application Load Balancer deve essere configurato per eliminare le intestazi oni http su Application Load Balancer deve essere configurato per eliminare le intestazi oni http non valide.
19 agosto 2024	Modifiche al titolo e ai controlli DMS.12 ElastiCache	Titoli di controllo modificati DMS.12 prima e ElastiCache.1 dopo ElastiCache.7. Abbiamo modificato questi titoli per rifletter e un cambio di nome nel servizio Amazon ElastiCache (Redis OSS).

Data di modifica	ID e titolo del controllo	Descrizione della modifica
15 agosto 2024	[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse	Config.1 verifica se AWS Config è abilitato, utilizza il ruolo collegato al servizio e registra le risorse per i controlli abilitati. Security Hub CSPM ha aggiunto un parametro di controllo personalizzato denominato `includeConfigServiceLinkedRoleCheck` Impostando questo parametro su `false`, è possibile scegliere di non verificare se AWS Config utilizza il ruolo collegato al servizio.
31 luglio 2024	[IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati	Il titolo di controllo modificato dai profili AWS IoT Core di sicurezza deve essere taggato ai profili AWS IoT Device Defender di sicurezza devono essere etichettati.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
29 luglio 2024	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM non supporta più `nodejs16.x` come parametro.
29 luglio 2024	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Questo controllo verifica se un cluster Amazon Elastic Kubernetes Service (Amazon EKS) viene eseguito su una versione di Kubernetes supportata. La versione più vecchia supportata è. `1.28`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
25 giugno 2024	[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse	Questo controllo verifica se AWS Config è abilitato , utilizza il ruolo collegato al servizio e registra le risorse per i controlli abilitati . Security Hub CSPM ha aggiornato il titolo del controllo per riflettere ciò che il controllo valuta.
14 giugno 2024	[RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch	Questo controllo verifica se un cluster Amazon Aurora MySQL DB è configurato per pubblicare log di audit su Amazon Logs. CloudWatch Security Hub CSPM ha aggiornato il controllo in modo che non generasse risultati per i cluster DB Aurora Serverless v1.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
11 giugno 2024	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Questo controllo verifica se un cluster Amazon Elastic Kubernetes Service (Amazon EKS) viene eseguito su una versione di Kubernetes supportata. La versione più vecchia supportata è. `1.27`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 giugno 2024	[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse	Questo controllo verifica se AWS Config è abilitato e la registrazione AWS Config delle risorse è attivata. In precedenza, il controllo produceva un `PASSED` risultato solo se si configura va la registrazione per tutte le risorse. Security Hub CSPM ha aggiornato il controllo per produrre un `PASSED` risultato quando la registraz ione è attivata per le risorse necessarie per i controlli abilitati . Il controllo è stato inoltre aggiornato per verificare se viene utilizzato il ruolo AWS Config collegato al servizio, che fornisce le autorizzazioni per registrare le risorse necessarie.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
8 maggio 2024	[S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata	Questo controllo verifica se un bucket con versione generica di Amazon S3 è abilitata l'eliminazione dell'autenticazione a più fattori (MFA). In precedenza, il controllo produceva una `FAILED` ricerca di bucket con una configurazione del ciclo di vita. Tuttavia, l'eliminazione MFA con controllo delle versioni non può essere abilitata su un bucket con una configurazione del ciclo di vita. Security Hub CSPM ha aggiornato il controllo per non produrre risultati per i bucket con una configura zione del ciclo di vita. La descrizione del controllo è stata aggiornata per rifletter e il comportamento corrente.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
2 maggio 2024	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Security Hub CSPM ha aggiornato la versione più vecchia supportata di Kubernetes su cui può essere eseguito il cluster Amazon EKS per produrre un risultato superato. La versione più vecchia attualmente supportat a è Kubernetes. `1.26`
30 aprile 2024	[CloudTrail.3] Almeno un CloudTrail percorso deve essere abilitato	Il titolo di controllo modificato da CloudTrail dovrebbe essere abilitato a Dovrebbe essere abilitato almeno un CloudTrail percorso. Questo controllo attualmente produce un `PASSED` risultato se un Account AWS ha almeno un CloudTrail percorso abilitato. Il titolo e la descrizione sono stati modificati per riflettere accuratam ente il comportamento attuale.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
29 aprile 2024	[AutoScaling.1] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB	La modifica del titolo di controllo dai gruppi Auto Scaling associati a un Classic Load Balancer dovrebbe utilizzare i controlli dello stato del bilanciamento del carico, mentre i gruppi Auto Scaling associati a un sistema di bilanciamento del carico dovrebbero utilizzare i controlli di integrità ELB. Questo controllo attualmente valuta Application, Gateway, Network e Classic Load Balancer. Il titolo e la descrizione sono stati modificati per riflettere accuratamente il comportamento corrente.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
19 aprile 2024	[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura	Il controllo verifica se AWS CloudTrail è abilitato e configurato con almeno un percorso multiregionale che include eventi di gestione di lettura e scrittura. In precedenza, il controllo generava erroneamente `PASSED` i risultati quando un account aveva CloudTrail abilitato e configurato almeno un percorso multiregionale, anche se nessun trail includeva eventi di gestione di lettura e scrittura. Il controllo ora genera un `PASSED` risultato solo quando CloudTrail è abilitato e configurato con almeno un percorso multiregionale che acquisisce gli eventi di gestione di lettura e scrittura.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[Athena.1] I gruppi di lavoro Athena devono essere crittografati quando sono inattivi	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard. I gruppi di lavoro Athena inviano i log ai bucket Amazon Simple Storage Service (Amazon S3). Amazon S3 ora fornisce la crittografia predefinita con chiavi gestite S3 (SS3-S3) su bucket S3 nuovi ed esistenti.
10 aprile 2024	[AutoScaling.4] La configurazione di avvio del gruppo Auto Scaling non deve avere un limite di hop di risposta ai metadati superiore a 1	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard. I limiti degli hop di risposta ai metadati per le istanze Amazon Elastic Compute Cloud (Amazon EC2) dipendono dal carico di lavoro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[CloudFormation.1] CloudFormation gli stack devono essere integrati con Simple Notification Service (SNS)	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard. L'integrazione degli AWS CloudFormation stack con gli argomenti di Amazon SNS non è più una best practice di sicurezza. Sebbene l'integrazione di CloudFormation stack importanti con argomenti SNS possa essere utile, non è necessaria per tutti gli stack.
10 aprile 2024	[CodeBuild.5] gli ambienti di CodeBuild progetto non dovrebbero avere la modalità privilegiata abilitata	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard. L'attivazione della modalità privilegiata in un CodeBuild progetto non comporta un rischio aggiuntivo per l'ambiente del cliente.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[IAM.20] Evita l'uso dell'utente root	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard. Lo scopo di questo controllo è coperto da un altro controllo,. [CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»
10 aprile 2024	[SNS.2] La registrazione dello stato di consegna deve essere abilitata per i messaggi di notifica inviati a un argomento	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard. La registrazione dello stato di consegna per gli argomenti SNS non è più una best practice di sicurezza. Sebbene la registrazione dello stato di consegna per importanti argomenti SNS possa essere utile, non è necessaria per tutti gli argomenti.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita	Security Hub CSPM ha rimosso questo controllo da AWS Foundational Security Best Practices and Service-Managed Standard:. AWS Control Tower Lo scopo di questo controllo è coperto da altri due controlli : e. [S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita S3.14[] I bucket S3 per uso generico devono avere il controllo delle versioni abilitato Questo controllo fa ancora parte del NIST SP 800-53 Rev. 5.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[] I bucket S3 per uso generico devono avere le notifiche degli eventi abilitate S3.11	Security Hub CSPM ha rimosso questo controllo da AWS Foundational Security Best Practices and Service-Managed Standard:. AWS Control Tower Sebbene ci siano alcuni casi in cui le notifiche di eventi per i bucket S3 sono utili, questa non è una best practice di sicurezza universale. Questo controllo fa ancora parte del NIST SP 800-53 Rev. 5.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[SNS.1] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS	Security Hub CSPM ha rimosso questo controllo da AWS Foundational Security Best Practices and Service-Managed Standard: . AWS Control Tower Per impostazione predefinita, SNS crittografa gli argomenti inattivi con la crittografia del disco. Per ulteriori informazioni, consulta Crittografia dei dati. L'utilizzo AWS KMS per crittografare gli argomenti non è più consigliato come best practice di sicurezza . Questo controllo fa ancora parte di NIST SP 800-53 Rev. 5.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
8 aprile 2024	[ELB.6] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata	Il titolo di controllo modificato dalla protezione da eliminazione di Application Load Balancer deve essere abilitato a Application, Gateway e Network Load Balancer dovrebbe avere la protezion e da eliminazione abilitata. Questo controllo attualmen te valuta Application, Gateway e Network Load Balancer. Il titolo e la descrizione sono stati modificati per riflettere accuratam ente il comportamento attuale.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
22 marzo 2024	[Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente	Il titolo di controllo modificato da Connessioni ai OpenSearch domini deve essere crittografato utilizzando TLS 1.2 a Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS. In precedenza, il controllo controllava solo se le connessioni ai OpenSearch domini utilizzavano TLS 1.2. Il controllo ora consente di determinare se i OpenSearch domini sono crittografati utilizzando la più recente politica di sicurezza TLS. `PASSED` Il titolo e la descrizione del controllo sono stati aggiornati per riflettere il comportamento corrente.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
22 marzo 2024	[ES.8] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS	Il titolo di controllo modificato da Connessioni ai domini Elasticsearch deve essere crittografato utilizzando TLS 1.2 a Connessioni ai domini Elasticsearch deve essere crittografato utilizzando la politica di sicurezza TLS più recente. In precedenza, il controllo controllava solo se le connessioni ai domini Elasticsearch utilizzavano TLS 1.2. Il controllo ora determina se i domini Elasticsearch sono crittografati utilizzando la più recente politica di sicurezza TLS. `PASSED` Il titolo e la descrizione del controllo sono stati aggiornati per riflettere il comportamento corrente.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate	Il titolo modificato dall'impostazione S3 Block Public Access deve essere abilitato ai bucket generici S3 devono avere le impostazioni di accesso pubblico a blocchi abilitate. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.2] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura	Il titolo modificato dei bucket S3 dovrebbe proibire l'accesso pubblico in lettura ai bucket S3 per uso generico e dovrebbe bloccare l'accesso pubblico in lettura. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.3] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura	Il titolo modificato dei bucket S3 dovrebbe proibire l'accesso pubblico in scrittura ai bucket S3 per uso generico e dovrebbe bloccare l'accesso pubblico in scrittura . Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS	Il titolo modificato dai bucket S3 dovrebbe richiedere le richieste di utilizzo di Secure Socket Layer, mentre i bucket S3 per uso generico dovrebber o richiedere richieste di utilizzo di SSL. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.6] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS	Il titolo modificato dalle autorizzazioni S3 concesse ad altre Account AWS in politiche bucket dovrebbe essere limitato alle policy dei bucket per uso generale di S3. Le policy relative ai bucket dovrebbero limitare l'accesso ad altri. Account AWS Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni	Il titolo modificato dei bucket S3 dovrebbe avere la replica tra regioni abilitata, mentre i bucket S3 per uso generico dovrebbero utilizzare la replica tra regioni. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni	Il titolo modificato dei bucket S3 dovrebbe avere la replica tra regioni abilitata, mentre i bucket S3 per uso generico dovrebbero utilizzare la replica tra regioni. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico	Il titolo modificato dall'impostazione S3 Block Public Access deve essere abilitato a livello di bucket, mentre i bucket S3 per uso generico devono bloccare l'accesso pubblico. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.9] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata	Il titolo modificato dalla registrazione degli accessi al server del bucket S3 deve essere abilitato in La registrazione dell'accesso al server deve essere abilitata per i bucket S3 per uso generico. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita	Il titolo modificato dai bucket S3 con il controllo delle versioni abilitato dovrebbe avere politiche del ciclo di vita configura te in bucket S3 per uso generico con il controllo delle versioni abilitato dovrebber o avere configura zioni del ciclo di vita. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate	Il titolo modificato dei bucket S3 dovrebbe avere le notifiche degli eventi abilitate , mentre i bucket S3 per uso generico dovrebbero avere le notifiche degli eventi abilitate. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.12] Gli ACL non devono essere utilizzat i per gestire l'accesso degli utenti ai bucket generici S3	Il titolo modificat o degli elenchi di controllo degli accessi (ACL) di S3 non deve essere utilizzato per gestire l'accesso degli utenti ai bucket, mentre gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket S3 per uso generico. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita	Il titolo modificato dei bucket S3 dovrebbe avere politiche del ciclo di vita configurate in base ai bucket S3 per uso generico e i bucket S3 dovrebbero avere configurazioni del ciclo di vita. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	S3.14[] I bucket S3 per uso generico devono avere il controllo delle versioni abilitato	Il titolo modificato dai bucket S3 dovrebbe utilizzare il controllo delle versioni, mentre i bucket S3 per uso generico dovrebbero avere il controllo delle versioni abilitato. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.15] I bucket generici S3 devono avere Object Lock abilitato	Il titolo modificato dai bucket S3 deve essere configura to per utilizzare Object Lock, mentre i bucket S3 per uso generico devono avere Object Lock abilitato. Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.17] I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys	Il titolo modificato dai bucket S3 deve essere crittogra fato con i bucket inattivi con i bucket S3 AWS KMS keys per uso generico con. AWS KMS keys Security Hub CSPM ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
7 marzo 2024	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `nodejs20.x` e `ruby3.3` come parametri.
22 febbraio 2024	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `dotnet8` come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 febbraio 2024	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Security Hub CSPM ha aggiornato la versione più vecchia supportata di Kubernetes su cui può essere eseguito il cluster Amazon EKS per produrre un risultato superato. La versione più vecchia attualmente supportata è Kubernetes. `1.25`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 gennaio 2024	[CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili	Il titolo modificato CodeBuild GitHub o gli URL del repository di origine Bitbucket devono utilizzare OAuth, mentre gli URL del repository di origine CodeBuild Bitbucket non devono contenere credenziali riservate. Security Hub CSPM ha rimosso la menzione di OAuth perché anche altri metodi di connessione possono essere sicuri. Security Hub CSPM ha rimosso la menzione GitHub perché non è più possibile avere un token di accesso personale o un nome utente e una password negli URL del repository di GitHub origine.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
8 gennaio 2024	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM non supporta più `go1.x` e `java8` come parametri perché si tratta di runtime ritirati.
29 dicembre 2023	[RDS.8] Le istanze DB RDS devono avere la protezione da eliminazione abilitata	RDS.8 verifica se un'istanza DB Amazon RDS che utilizza uno dei motori di database supportati ha la protezione da eliminazione abilitata. Security Hub CSPM ora supporta `custom-oracle-ee` e `oracle-se2-cdb` come motori di database. `oracle-ee-cdb`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
22 dicembre 2023	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `java21` e `python3.12` come parametri. Security Hub CSPM non supporta più `ruby2.7` come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
15 dicembre 2023	[CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato	CloudFront.1 verifica se una CloudFront distribuzione Amazon ha un oggetto root predefinito configurato. Security Hub CSPM ha ridotto la severità di questo controllo da CRITICAL a HIGH perché l'aggiunt a dell'oggetto root predefinito è una raccomandazione che dipende dall'appl icazione dell'utente e dai requisiti specifici.
5 dicembre 2023	[EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22	Il titolo di controllo modificato dai gruppi di sicurezza non dovrebbe consentir e l'ingresso a partire dalla versione 0.0.0. 0/0 la porta 22 ai gruppi di sicurezza non dovrebbe consentire l'ingresso da 0.0.0. 0/0 o: :/0 alla porta 22.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 dicembre 2023	[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389	Titolo di controllo modificato da Assicura che nessun gruppo di sicurezza consenta l'ingress o a partire dalla versione 0.0.0. 0/0 la porta 3389 ai gruppi di sicurezza non dovrebbe consentir e l'ingresso da 0.0.0. 0/0 o: :/0 alla porta 3389.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 dicembre 2023	[RDS.9] Le istanze DB RDS devono pubblicare i log in Logs CloudWatch	Il titolo di controllo modificato dalla registrazione del database deve essere abilitato. Le istanze DB RDS devono pubblicare i registri nei registri. CloudWatch Security Hub CSPM ha rilevato che questo controllo verifica solo se i log sono pubblicati su Amazon CloudWatch Logs e non verifica se i log RDS sono abilitati. Il controllo rileva se le istanze DB RDS sono configurate per pubblicare log su Logs. PASSED CloudWatch Il titolo del controllo è stato aggiornato per riflettere il comportamento corrente.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 dicembre 2023	[EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata	Questo controllo verifica se i cluster Amazon EKS hanno abilitato la registrazione di audit. La AWS Config regola utilizzata da Security Hub CSPM per valutare questo controllo è stata modificata da `aeks-cluster-logging-enabled` . `eks-cluster-log-enabled`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
17 novembre 2023	[EC2.19] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio	EC2.19 verifica se il traffico in entrata senza restrizioni per un gruppo di sicurezza è accessibile alle porte specificate considerate ad alto rischio. Security Hub CSPM ha aggiornato questo controllo per tenere conto degli elenchi di prefissi gestiti quando vengono forniti come origine per una regola del gruppo di sicurezza. Il controllo rileva se gli elenchi di prefissi contengono le stringhe '0.0.0. 0/0' o ': :/0'. `FAILED`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 novembre 2023	[CloudWatch.15] gli CloudWatch allarmi dovrebbero avere azioni specificate configurate	Il titolo di controllo modificato dagli CloudWatch allarmi dovrebbe avere un'azione configura ta per lo stato CloudWatch ALARM, mentre gli allarmi dovrebbero avere delle azioni specifica te configurate.
16 novembre 2023	[CloudWatch.16] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato	Il titolo di controllo modificato dei gruppi di CloudWatch log deve essere conservato per almeno 1 anno, mentre i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 novembre 2023	[Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità	Il titolo di controllo modificato dalle funzioni VPC Lambda deve funzionare in più di una zona di disponibilità, mentre le funzioni VPC Lambda devono funzionare in più zone di disponibi lità.
16 novembre 2023	[AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata	La modifica del titolo di controllo da AWS AppSync dovrebbe avere la registrazione a livello di richiesta e di campo attivata a dovrebbe avere la registrazione a livello di campo abilitata .AWS AppSync
16 novembre 2023	[EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici	Il titolo di controllo modificato dai nodi master MapReduce del cluster Amazon Elastic non dovrebbe avere indirizzi IP pubblici, mentre i nodi primari del cluster Amazon EMR non dovrebbero avere indirizzi IP pubblici.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 novembre 2023	[Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico	Il titolo di controllo modificato dai OpenSearch domini dovrebbe essere in un VPC, in quanto i domini non dovrebber o essere accessibi li OpenSearch al pubblico.
16 novembre 2023	[ES.2] I domini Elasticsearch non devono essere accessibili al pubblico	Il titolo di controllo modificato dai domini Elasticsearch dovrebbe essere in un VPC, mentre i domini Elasticsearch non dovrebbero essere accessibili al pubblico.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
31 ottobre 2023	[ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch	ES.4 verifica se i domini Elasticsearch sono configurati per inviare log di errori ad Amazon CloudWatch Logs. Il controllo in precedenza produceva una `PASSED` ricerca per un dominio Elasticsearch con tutti i log configurati per l'invio a CloudWatch Logs. Security Hub CSPM ha aggiornato il controllo per produrre un `PASSED` risultato solo per un dominio Elasticsearch configurato per inviare i log degli errori ai registri. CloudWatch Il controllo è stato inoltre aggiornato per escludere dalla valutazione le versioni di Elasticsearch che non supportano i log degli errori.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 ottobre 2023	[EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22	EC2.13 verifica se i gruppi di sicurezza consentono l'accesso illimitato in ingresso alla porta 22. Security Hub CSPM ha aggiornato questo controllo per tenere conto degli elenchi di prefissi gestiti quando vengono forniti come origine per una regola del gruppo di sicurezza . Il controllo rileva se gli elenchi di `FAILED` prefissi contengono le stringhe '0.0.0. 0/0' o ': :/0'.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 ottobre 2023	[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389	EC2.14 verifica se i gruppi di sicurezza consentono l'accesso illimitato in ingresso alla porta 3389. Security Hub CSPM ha aggiornato questo controllo per tenere conto degli elenchi di prefissi gestiti quando vengono forniti come origine per una regola del gruppo di sicurezza . Il controllo rileva se gli elenchi di `FAILED` prefissi contengono le stringhe '0.0.0. 0/0' o ': :/0'.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 ottobre 2023	[EC2.18] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate	EC2.18 verifica se i gruppi di sicurezza in uso consentono il traffico in entrata senza restrizioni. Security Hub CSPM ha aggiornato questo controllo per tenere conto degli elenchi di prefissi gestiti quando vengono forniti come origine per una regola del gruppo di sicurezza . Il controllo rileva se gli elenchi di `FAILED` prefissi contengono le stringhe '0.0.0. 0/0' o ': :/0'.
16 ottobre 2023	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ciascuna lingua. Security Hub CSPM ora supporta `python3.11` come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
4 ottobre 2023	[S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni	Security Hub CSPM ha aggiunto il parametro `ReplicationType` con un valore pari `CROSS-REGION` a per garantire che nei bucket S3 sia abilitata la replica tra regioni anziché la replica nella stessa regione.
27 settembre 2023	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Security Hub CSPM ha aggiornato la versione più vecchia supportata di Kubernetes su cui può essere eseguito il cluster Amazon EKS per produrre un risultato superato. La versione più vecchia attualmente supportat a è Kubernetes. `1.24`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
20 settembre 2023	[CloudFront.2] le CloudFront distribuzioni devono avere l'identità di accesso all'origine abilitata	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard. Altrimenti, consulta [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine. Il controllo degli accessi Origin è l'attuale best practice di sicurezza. Questo controllo verrà rimosso dalla documentazione entro 90 giorni.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
20 settembre 2023	[EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi	Security Hub CSPM ha rimosso questo controllo da AWS Foundational Security Best Practices (FSBP) e National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5. Service-Managed AWS Control Tower Fa ancora parte di Standard:. Questo controllo produce un risultato positivo se i gruppi di sicurezza sono collegati a istanze EC2 o a un'interfaccia di rete elastica. Tuttavia, in alcuni casi d'uso, i gruppi di sicurezza non collegati non rappresentano un rischio per la sicurezza. Puoi utilizzare altri controlli EC2 EC2.2, come,, EC2.13 EC2.14, e EC2.19 —per monitorare i tuoi EC2.18 gruppi di sicurezza.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
20 settembre 2023	[EC2.29] Le istanze EC2 devono essere avviate in un VPC	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard. Amazon EC2 ha migrato le EC2-Classic istanze su un VPC. Questo controllo verrà rimosso dalla documentazione entro 90 giorni.
20 settembre 2023	[S3.4] I bucket S3 devono avere la crittografia lato server abilitata	Security Hub CSPM ha ritirato questo controllo e lo ha rimosso da tutti gli standard. Amazon S3 ora fornisce la crittografia predefinita con chiavi gestite S3 (SS3-S3) su bucket S3 nuovi ed esistenti . Le impostazioni di crittografia sono invariate per i bucket esistenti crittografati con o crittografia lato server. SS3-S3 SS3-KMS Questo controllo verrà rimosso dalla documentazione tra 90 giorni.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 settembre 2023	[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita	Titolo di controllo modificato da Il gruppo di sicurezza predefinito VPC non dovrebbe consentir e il traffico in entrata e in uscita ai gruppi di sicurezza predefini ti VPC non dovrebbe consentire il traffico in entrata o in uscita.
14 settembre 2023	[IAM.9] L'MFA deve essere abilitata per l'utente root	Il titolo di controllo modificato da Virtual MFA deve essere abilitato per l'utente root a MFA deve essere abilitato per l'utente root.
14 settembre 2023	[RDS.19] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici del cluster	Titolo di controllo modificato da Un abbonamento per le notifiche di eventi RDS deve essere configurato per gli eventi critici del cluster a Gli abbonamenti di notifica degli eventi RDS esistenti devono essere configurati per gli eventi critici del cluster.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 settembre 2023	[RDS.20] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici delle istanze di database	Titolo di controllo modificato da Un abbonamento alle notifiche di eventi RDS deve essere configurato per gli eventi critici delle istanze di database Gli abbonamenti di notifica degli eventi RDS esistenti devono essere configurati per gli eventi critici delle istanze di database.
14 settembre 2023	[WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione	Il titolo di controllo modificato da una regola regionale WAF dovrebbe avere almeno una condizione, mentre le regole regionali AWS WAF classiche dovrebbero avere almeno una condizione.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 settembre 2023	[WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola	Il titolo di controllo modificato da Un gruppo di regole regionali WAF dovrebbe avere almeno una regola, mentre i gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola.
14 settembre 2023	[WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole	Titolo di controllo modificato da Un ACL web regionale WAF dovrebbe avere almeno una regola o un gruppo di regole a un ACL web regionale AWS WAF classico gli ACL web regionali classici dovrebber o avere almeno una regola o un gruppo di regole.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 settembre 2023	[WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione	Il titolo di controllo modificato da Una regola globale WAF dovrebbe avere almeno una condizione a Le regole globali AWS WAF Classic dovrebbero avere almeno una condizione.
14 settembre 2023	[WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola	Il titolo di controllo modificato da Un gruppo di regole globale WAF dovrebbe avere almeno una regola, mentre i gruppi di regole globali AWS WAF Classic dovrebbero avere almeno una regola.
14 settembre 2023	[WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole	Titolo di controllo modificato da Un ACL web globale WAF dovrebbe avere almeno una regola o un gruppo di regole a Gli ACL web globali AWS WAF classici dovrebbero avere almeno una regola o un gruppo di regole.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 settembre 2023	[WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole	Il titolo di controllo modificato da Un ACL web WAFv2 deve avere almeno una regola o un gruppo di regole, mentre gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole.
14 settembre 2023	[WAF.11] AWS WAF la registrazione ACL web deve essere abilitata	Il titolo di controllo modificato dalla registrazione ACL Web AWS WAF v2 deve essere attivato alla registrazione ACL Web deve essere abilitata.AWS WAF

Data di modifica	ID e titolo del controllo	Descrizione della modifica
20 luglio 2023	[S3.4] I bucket S3 devono avere la crittografia lato server abilitata	S3.4 verifica se un bucket Amazon S3 ha la crittografia lato server abilitata o se la policy del bucket S3 nega esplicita mente le richieste senza crittografia lato server. `PutObject` Security Hub CSPM ha aggiornato questo controllo per includere la crittografia lato server a doppio livello con chiavi KMS (). DSSE-KMS Il controllo produce un risultato superato quando un bucket S3 viene crittografato con, o. SSE-S3 SSE-KMS DSSE-KMS

Data di modifica	ID e titolo del controllo	Descrizione della modifica
17 luglio 2023	[S3.17] I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys	S3.17 verifica se un bucket Amazon S3 è crittografato con un. AWS KMS key Security Hub CSPM ha aggiornato questo controllo per includere la crittografia lato server a doppio livello con chiavi KMS (). DSSE-KMS Il controllo produce un risultato superato quando un bucket S3 viene crittografato con o. SSE-KMS DSSE-KMS
9 giugno 2023	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	EKS.2 verifica se un cluster Amazon EKS è in esecuzione su una versione di Kubernetes supportata. La versione più vecchia supportata è ora. `1.23`

Data di modifica	ID e titolo del controllo	Descrizione della modifica
9 giugno 2023	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `ruby3.2` come parametro.
5 giugno 2023	[APIGateway.5] I dati della cache dell'API REST di API Gateway devono essere crittografati quando sono inattivi	APIGateway.5.checks se tutti i metodi nelle fasi dell'API REST di Amazon API Gateway sono crittografati a riposo. Security Hub CSPM ha aggiornato il controllo per valutare la crittografia di un particolare metodo solo quando la memorizzazione nella cache è abilitata per quel metodo.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
18 maggio 2023	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `java17` come parametro.
18 maggio 2023	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM non supporta più `nodejs12.x` come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
23 aprile 2023	[ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate	ECS.10 verifica se i servizi Amazon ECS Fargate eseguono l'ultima versione della piattaforma Fargate. I clienti possono implement are Amazon ECS tramite ECS direttame nte o utilizzando. CodeDeploy Security Hub CSPM ha aggiornato questo controllo per produrre risultati Passed da utilizzare CodeDeploy per distribuire i servizi ECS Fargate.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
20 aprile 2023	[S3.6] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS	S3.6 verifica se una policy sui bucket di Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) impedisce Account AWS ai principali di eseguire azioni negate sulle risorse nel bucket S3. Security Hub CSPM ha aggiornato il controllo per tenere conto dei condizionali in una policy bucket.
18 aprile 2023	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM ora supporta `python3.10` come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
18 aprile 2023	[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub CSPM non supporta più `dotnetcore3.1` come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
17 aprile 2023	[RDS.11] Le istanze RDS devono avere i backup automatici abilitati	RDS.11 verifica se sulle istanze Amazon RDS sono abilitati i backup automatic i, con un periodo di conservazione dei backup maggiore o uguale a sette giorni. Security Hub CSPM ha aggiornat o questo controllo per escludere le repliche di lettura dalla valutazione, poiché non tutti i motori supportano i backup automatic i sulle repliche di lettura. Inoltre, RDS non offre la possibili tà di specificare un periodo di conservaz ione dei backup durante la creazione di repliche di lettura. Le repliche di lettura vengono create con un periodo di conservazione dei backup di 0 default.

Controlli CSPM Security Hub per Account AWS

Questi controlli CSPM di Security Hub valutano. Account AWS

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-2, Profilo CRI v2. 2/DE. AE-06.01, Profilo CRI v2. 2/RS. CO-02.01, Profilo CRI v2. 2/RS. CO-02.03

Categoria: Identificazione > Configurazione delle risorse

Gravità: media

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `security-account-information-provided`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un account Amazon Web Services (AWS) dispone di informazioni di contatto di sicurezza. Il controllo fallisce se non vengono fornite informazioni di contatto di sicurezza per l'account.

I contatti di sicurezza alternativi consentono di contattare un'altra persona in merito AWS a problemi relativi al tuo account nel caso in cui tu non sia disponibile. Le notifiche possono provenire da Supporto o da altri Servizio AWS team su argomenti relativi alla sicurezza associati al tuo utilizzo. Account AWS

Correzione

Per aggiungere un contatto alternativo come contatto di sicurezza al tuo Account AWS, consulta Aggiornare i contatti alternativi per te Account AWS nella Guida di riferimento per la gestione dell'AWS account.

[Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/ID. AM-08.02

Gravità: alta

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `account-part-of-organizations`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un Account AWS fa parte di un'organizzazione gestita tramite AWS Organizations. Il controllo ha esito negativo se l'account non fa parte di un'organizzazione.

Organizations ti aiuta a gestire centralmente il tuo ambiente man mano che ridimensioni i carichi di lavoro. AWSÈ possibile utilizzarne più Account AWS di uno per isolare i carichi di lavoro con requisiti di sicurezza specifici o per conformarsi a framework come HIPAA o PCI. Creando un'organizzazione, puoi amministrare più account come una singola unità e gestirne centralmente l'accesso, le risorse e le regioni. Servizi AWS

Correzione

Per creare una nuova organizzazione e Account AWS aggiungerla automaticamente, consulta Creazione di un'organizzazione nella Guida per l'AWS Organizations utente. Per aggiungere account a un'organizzazione esistente, vedi Invitare un utente Account AWS a entrare a far parte della tua organizzazione nella Guida per l'AWS Organizations utente.

Controlli CSPM Security Hub per AWS Amplify

Questi controlli CSPM di Security Hub valutano il AWS Amplify servizio e le risorse. I controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Amplify.1] Le app Amplify devono essere taggate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Amplify::App`

Regola AWS Config : amplify-app-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un' AWS Amplify app ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo ha esito negativo se l'app non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'app non dispone di chiavi di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un' AWS Amplify app, consulta il supporto per il tagging delle risorse nella Guida per l'utente AWS Amplify di hosting.

[Amplify.2] I rami Amplify devono essere etichettati

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Amplify::Branch`

Regola AWS Config : amplify-branch-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un AWS Amplify ramo ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo ha esito negativo se il ramo non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il ramo non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le

risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a una AWS Amplify filiale, consulta il supporto per l'etichettatura delle risorse nella Guida per l'utente AWS Amplify di hosting.

Controlli CSPM del Security Hub per Amazon API Gateway

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse di Amazon API Gateway. I controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[APIGateway.1] API Gateway REST e la registrazione dell'esecuzione dell' WebSocket API devono essere abilitati

Requisiti correlati: 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), CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa:`AWS::ApiGateway::Stage`, `AWS::ApiGatewayV2::Stage`

Regola AWS Config : api-gw-execution-logging-enabled

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`loggingLevel`	Livello di logging	Enum	`ERROR`, `INFO`	`No default value`

Questo controllo verifica se la registrazione è abilitata in tutte le fasi di un'API o REST di Amazon WebSocket API Gateway. Il controllo fallisce se `loggingLevel` non lo è `ERROR` o `INFO` per tutte le fasi dell'API. A meno che non si forniscano valori di parametro personalizzati per indicare che un tipo di registro specifico deve essere abilitato, Security Hub CSPM produce un risultato valido se il livello di registrazione è o. `ERROR` `INFO`

API Gateway WebSocket REST o le fasi API devono avere i log pertinenti abilitati. La registrazione REST e l'esecuzione delle WebSocket API di API Gateway forniscono registrazioni dettagliate delle richieste effettuate alle fasi REST e API di WebSocket API Gateway. Le fasi includono le risposte di backend di integrazione delle API, le risposte di autorizzazione Lambda e gli endpoint per `requestId` l' AWS integrazione.

Correzione

Per abilitare la registrazione per le operazioni WebSocket REST e API, consulta Configurare la registrazione delle CloudWatch API utilizzando la console API Gateway nella API Gateway Developer Guide.

[APIGateway.2] Le fasi API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend

Requisiti correlati: 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, Profilo CRI v2. 2/PR. PS-01.06, Profilo CRI v2. 2/PR. PS-01.07

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ApiGateway::Stage`

Regola AWS Config : api-gw-ssl-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le fasi API REST di Amazon API Gateway hanno certificati SSL configurati. I sistemi di backend utilizzano questi certificati per autenticare che le richieste in entrata provengano da API Gateway.

Le fasi API REST di API Gateway devono essere configurate con certificati SSL per consentire ai sistemi di backend di autenticare che le richieste provengono da API Gateway.

Correzione

Per istruzioni dettagliate su come generare e configurare i certificati SSL API REST API Gateway, consulta Generare e configurare un certificato SSL per l'autenticazione di backend nella Guida per sviluppatori di API Gateway.

[APIGateway.3] Le fasi API REST di API Gateway dovrebbero avere AWS X-Ray tracciamento abilitato

Requisiti correlati: NIST.800-53.r5 CA-7, CRI Profile v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-04.02

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa: `AWS::ApiGateway::Stage`

Regola AWS Config : api-gw-xray-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il tracciamento AWS X-Ray attivo è abilitato per le fasi dell'API REST di Amazon API Gateway.

X-Ray il tracciamento attivo consente una risposta più rapida ai cambiamenti delle prestazioni nell'infrastruttura sottostante. Le variazioni delle prestazioni potrebbero comportare una mancanza di disponibilità dell'API. X-Rayactive tracing fornisce metriche in tempo reale delle richieste degli utenti che fluiscono attraverso le operazioni dell'API REST dell'API Gateway e i servizi connessi.

Correzione

Per istruzioni dettagliate su come abilitare il tracciamento X-Ray attivo per le operazioni API REST di API Gateway, consulta il supporto per il tracciamento attivo di Amazon API Gateway AWS X-Ray nella AWS X-Ray Developer Guide.

[APIGateway.4] API Gateway deve essere associato a un ACL Web WAF

Requisiti correlati: NIST.800-53.r5 AC-4 (21), CRI Profile v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.03

Categoria: Proteggi > Servizi di protezione

Gravità: media

Tipo di risorsa: `AWS::ApiGateway::Stage`

Regola AWS Config : api-gw-associated-with-waf

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una fase API Gateway utilizza una lista di controllo degli accessi AWS WAF Web (ACL). Questo controllo ha esito negativo se un ACL AWS WAF Web non è collegato a uno stadio REST API Gateway.

AWS WAF è un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web e le API dagli attacchi. Consente di configurare un ACL, ovvero un insieme di regole che consentono,

bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. Assicurati che la fase API Gateway sia associata a un ACL AWS WAF Web per proteggerla da attacchi dannosi.

Correzione

Per informazioni su come utilizzare la console API Gateway per associare un ACL web AWS WAF regionale a una fase API Gateway API esistente, consulta Using AWS WAF to protect your API nella API Gateway Developer Guide.

[APIGateway.5] I dati della cache dell'API REST di API Gateway devono essere crittografati quando sono inattivi

Requisiti correlati: 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, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: `AWS::ApiGateway::Stage`

AWS Config regola: `api-gw-cache-encrypted` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se tutti i metodi nelle fasi API REST di API Gateway con cache abilitata sono crittografati. Il controllo ha esito negativo se un metodo in una fase API REST API Gateway è configurato per la cache e la cache non è crittografata. Security Hub CSPM valuta la crittografia di un particolare metodo solo quando la memorizzazione nella cache è abilitata per quel metodo.

La crittografia dei dati inattivi riduce il rischio di accesso ai dati archiviati su disco da parte di un utente non autenticato. AWS Aggiunge un altro set di controlli di accesso per limitare la capacità degli utenti non autorizzati di accedere ai dati. Ad esempio, sono necessarie le autorizzazioni API per decrittografare i dati prima che possano essere letti.

Le cache delle API REST di API Gateway devono essere crittografate quando sono inattive per un ulteriore livello di sicurezza.

Correzione

Per configurare la memorizzazione nella cache delle API per una fase, consulta Abilita la memorizzazione nella cache di Amazon API Gateway nella API Gateway Developer Guide. In Impostazioni cache, scegli Crittografa i dati della cache.

[APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione

Requisiti correlati: 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

Categoria: Protezione > Gestione sicura degli accessi

Gravità: media

Tipo di risorsa: `AWS::ApiGatewayV2::Route`

Regola AWS Config : api-gwv2-authorization-type-configured

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`authorizationType`	Tipo di autorizzazione dei percorsi API	Enum	`AWS_IAM`, `CUSTOM`, `JWT`	Nessun valore predefinito

Questo controllo verifica se le route Amazon API Gateway hanno un tipo di autorizzazione. Il controllo fallisce se la route API Gateway non ha alcun tipo di autorizzazione. Facoltativamente, puoi fornire un valore di parametro personalizzato se desideri che il controllo passi solo se la route utilizza il tipo di autorizzazione specificato nel `authorizationType` parametro.

API Gateway supporta più meccanismi per controllare e gestire l'accesso all'API. Specificando un tipo di autorizzazione, puoi limitare l'accesso all'API solo agli utenti o ai processi autorizzati.

Correzione

Per impostare un tipo di autorizzazione per le API HTTP, consulta Controllare e gestire l'accesso a un'API HTTP in API Gateway nella API Gateway Developer Guide. Per impostare un tipo di autorizzazione per le WebSocket API, consulta Controllare e gestire l'accesso a un' WebSocket API in API Gateway nella API Gateway Developer Guide.

[APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages

Requisiti correlati: 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), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::ApiGatewayV2::Stage`

Regola AWS Config : api-gwv2-access-logs-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se nelle fasi di Amazon API Gateway V2 è configurata la registrazione degli accessi. Questo controllo fallisce se le impostazioni del log di accesso non sono definite.

I log di accesso all'API Gateway forniscono informazioni dettagliate su chi ha effettuato l'accesso all'API e su come il chiamante ha effettuato l'accesso all'API. Questi log sono utili per applicazioni quali audit di sicurezza e accesso e indagini forensi. Abilita questi log di accesso per analizzare i modelli di traffico e risolvere i problemi.

Per ulteriori best practice, consulta Monitoring REST API nella API Gateway Developer Guide.

Correzione

Per configurare la registrazione degli accessi, consulta Configurare la registrazione delle CloudWatch API utilizzando la console API Gateway nella Guida per sviluppatori di API Gateway.

[APIGateway.10] Le integrazioni API Gateway V2 devono utilizzare HTTPS per le connessioni private

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ApiGatewayV2::Integration`

Regola AWS Config : apigatewayv2-integration-private-https-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'integrazione API Gateway V2 ha HTTPS abilitato per le connessioni private. Il controllo fallisce se per una connessione privata non è configurato TLS.

I collegamenti VPC collegano l'API Gateway alle risorse private. Sebbene i collegamenti VPC creino connettività privata, non crittografano intrinsecamente i dati. La configurazione di TLS garantisce l'uso di HTTPS per la crittografia end-to-end dal client tramite API Gateway al backend. Senza TLS, il traffico API sensibile scorre in modo non crittografato tra le connessioni private. La crittografia HTTPS protegge il traffico attraverso le connessioni private dall'intercettazione dei dati, dagli attacchi man-in-the-middle e dall'esposizione delle credenziali.

Correzione

Per abilitare la crittografia in transito per le connessioni private in un'integrazione API Gateway v2, consulta Aggiornare un'integrazione privata nella Amazon API Gateway Developer Guide. Configura la configurazione TLS in modo che l'integrazione privata utilizzi il protocollo HTTPS.

[APIGateway.11] I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate

Categoria: Protezione > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ApiGateway::DomainName`

Regola AWS Config : apigateway-domain-name-tls-check

Tipo di pianificazione: modifica attivata

Parametri:

- `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` (non personalizzabile)

Questo controllo verifica se un nome di dominio API Gateway è configurato per crittografare i dati in transito utilizzando una politica di sicurezza consigliata. Il controllo fallisce se il nome di dominio API Gateway non è configurato per utilizzare una politica di sicurezza consigliata.

Questo controllo genera una `FAILED` ricerca per i nomi di dominio personalizzati collegati alle API HTTP. Se hai un caso d'uso legittimo per le API HTTP, puoi sopprimere il risultato.

Una policy di sicurezza è una combinazione predefinita di versione TLS minima e suite di crittografia offerta da Gateway API. Quando i client stabiliscono un handshake TLS sull'API o sul nome di dominio personalizzato, la policy di sicurezza applica la versione di TLS e il pacchetto di crittografia accettato da API Gateway. Le policy di sicurezza proteggono le API e i nomi di dominio personalizzati da problemi di sicurezza della rete, ad esempio manomissioni e eavesdropping tra un client e un server. L'utilizzo di una politica di sicurezza consigliata aiuta a garantire che i nomi di dominio API Gateway utilizzino configurazioni TLS moderne e sicure che proteggono i dati in transito tra i client e l'API.

Correzione

Per aggiornare la policy di sicurezza TLS per un nome di dominio API Gateway, consulta Come modificare una politica di sicurezza nella Amazon API Gateway Developer Guide.

Controlli CSPM Security Hub perAWS AppConfig

Questi controlli CSPM di Security Hub valutano il AWS AppConfig servizio e le risorse.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::AppConfig::Application`

Regola AWS Config: `appconfig-application-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un'AWS AppConfigapplicazione dispone di tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se l'applicazione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'applicazione non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un'AWS AppConfigapplicazione, consulta l'AWS AppConfigAPI TagResourceReference.

[AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::AppConfig::ConfigurationProfile`

Regola AWS Config: `appconfig-configuration-profile-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un profilo AWS AppConfig di configurazione ha tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se il profilo di configurazione

non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il profilo di configurazione non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un profilo di AWS AppConfig configurazione, consulta l'AWS AppConfigAPI TagResourceReference.

[AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::AppConfig::Environment`

Regola AWS Config: `appconfig-environment-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un AWS AppConfig ambiente ha tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se l'ambiente non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'ambiente non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un AWS AppConfig ambiente, consulta l'AWS AppConfigAPI TagResourceReference.

[AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::AppConfig::ExtensionAssociation`

Regola AWS Config: `appconfig-extension-association-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un'associazione di AWS AppConfig estensioni contiene tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se l'associazione di estensione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'associazione di estensione non è etichettata

con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un'associazione di AWS AppConfig estensioni, consulta l'AWS AppConfigAPI TagResourceReference.

Controlli CSPM Security Hub per Amazon AppFlow

Questi controlli CSPM di Security Hub valutano il AppFlow servizio e le risorse Amazon.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[AppFlow.1] I AppFlow flussi Amazon devono essere etichettati

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::AppFlow::Flow`

Regola AWS Config : `appflow-flow-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un AppFlow flusso Amazon ha tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se il flusso non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il flusso non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per

ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un AppFlow flusso Amazon, consulta la sezione Creazione di flussi in Amazon AppFlow nella Amazon AppFlow User Guide.

Controlli CSPM Security Hub per AWS App Runner

Questi AWS Security Hub CSPM controlli valutano il AWS App Runner servizio e le risorse. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[AppRunner.1] I servizi App Runner devono essere etichettati

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::AppRunner::Service`

Regola AWS Config : apprunner-service-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un AWS App Runner servizio dispone di tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se il servizio App Runner non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il servizio App Runner non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per informazioni sull'aggiunta di tag a un AWS App Runner servizio, consulta l'AWS App Runner API TagResourceReference.

[AppRunner.2] I connettori VPC App Runner devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::AppRunner::VpcConnector`

Regola AWS Config : apprunner-vpc-connector-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un connettore AWS App Runner VPC ha tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se il connettore VPC non ha alcuna chiave tag o se non ha tutte le chiavi specificate nel parametro. `requiredKeyTags` Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se il connettore VPC non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse.

L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per informazioni sull'aggiunta di tag a un connettore AWS App Runner VPC, consulta l'AWS App Runner API TagResourceReference.

Controlli CSPM Security Hub per AWS AppSync

Questi controlli CSPM di Security Hub valutano il AWS AppSync servizio e le risorse.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata

Requisiti correlati: PCI DSS v4.0. 1/10.4.2, Profilo CRI v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/PR. PS-04.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::AppSync::GraphQLApi`

Regola AWS Config : `appsync-logging-enabled`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`fieldLoggingLevel`	Livello di registrazione del campo	Enum	`ERROR`, `ALL`, `INFO`, `DEBUG`	No `default value`	

Questo controllo verifica se un' AWS AppSync API ha attivato la registrazione a livello di campo. Il controllo ha esito negativo se il livello di registro del resolver del campo è impostato su Nessuno. A meno che non si forniscano valori di parametro personalizzati per indicare che un tipo di registro specifico deve essere abilitato, Security Hub CSPM produce un risultato valido se il campo resolver log level è o. `ERROR` `ALL`

Puoi usare il logging e i parametri per identificare e ottimizzare le query GraphQL, oltre che per risolvere i relativi problemi. L'attivazione della registrazione per AWS AppSync GraphQL consente di ottenere informazioni dettagliate sulle richieste e le risposte delle API, identificare e rispondere ai problemi e rispettare i requisiti normativi.

Correzione

Per attivare la registrazione per AWS AppSync, consulta Setup and configuration nella Developer Guide.AWS AppSync

[AppSync.4] AWS AppSync Le API GraphQL devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::AppSync::GraphQLApi`

AWS Config regola: `tagged-appsync-graphqlapi` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un'API AWS AppSync GraphQL ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'API GraphQL non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se l'API GraphQL non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'API AWS AppSync GraphQL, consulta l'AWS AppSync API TagResourceReference.

[AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API

Requisiti correlati: 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 Profile v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-03.01

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: alta

Tipo di risorsa: `AWS::AppSync::GraphQLApi`

Regola AWS Config : `appsync-authorization-check`

Tipo di pianificazione: modifica attivata

Parametri:

- `AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS` (non personalizzabile)

Questo controllo verifica se l'applicazione utilizza una chiave API per interagire con un'API AWS AppSync GraphQL. Il controllo fallisce se un'API AWS AppSync GraphQL è autenticata con una chiave API.

Una chiave API è un valore codificato nell'applicazione che viene generato dal AWS AppSync servizio quando si crea un endpoint GraphQL non autenticato. Se questa chiave API è compromessa, l'endpoint è vulnerabile agli accessi involontari. A meno che tu non supporti un'applicazione o un sito Web accessibili al pubblico, non consigliamo di utilizzare una chiave API per l'autenticazione.

Correzione

Per impostare un'opzione di autorizzazione per l'API AWS AppSync GraphQL, consulta Autorizzazione e autenticazione nella Guida per gli AWS AppSync sviluppatori.

Controlli CSPM del Security Hub per Amazon Athena

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse di Amazon Athena. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Athena.2] I cataloghi di dati Athena devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Athena::DataCatalog`

AWS Config regola: `tagged-athena-datacatalog` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un catalogo dati Amazon Athena contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il catalogo dati non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e

fallisce se il catalogo dati non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un catalogo di dati Athena, consulta Tagging Athena resources nella Amazon Athena User Guide.

[Athena.3] I gruppi di lavoro Athena devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Athena::WorkGroup`

AWS Config regola: `tagged-athena-workgroup` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un gruppo di lavoro Amazon Athena dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gruppo di lavoro non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di lavoro non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gruppo di lavoro Athena, consulta Aggiungere ed eliminare tag su un singolo gruppo di lavoro nella Amazon Athena User Guide.

[Athena.4] I gruppi di lavoro Athena dovrebbero avere la registrazione abilitata

Requisiti correlati: CRI Profile v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/PR. IR-04.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::Athena::WorkGroup`

Regola AWS Config : athena-workgroup-logging-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo di lavoro Amazon Athena ha la registrazione abilitata. Il controllo fallisce se il gruppo di lavoro non ha la registrazione abilitata.

I registri di controllo tengono traccia e monitorano le attività del sistema. Forniscono una registrazione degli eventi che può aiutarvi a rilevare le violazioni della sicurezza, indagare sugli incidenti e rispettare le normative. I registri di controllo migliorano anche la responsabilità e la trasparenza complessive dell'organizzazione.

Correzione

Per informazioni sull'abilitazione della registrazione per un gruppo di lavoro Athena, consulta CloudWatch Enable query metrics in Athena nella Amazon Athena User Guide.

Controlli CSPM Security Hub per AWS Backup

Questi controlli CSPM di Security Hub valutano il AWS Backup servizio e le risorse.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi

Requisiti correlati: NIST.800-53.r5 CP-9 (8) NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. DS-11.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::Backup::RecoveryPoint`

Regola AWS Config : `backup-recovery-point-encrypted`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un punto di AWS Backup ripristino è crittografato quando è inattivo. Il controllo fallisce se il punto di ripristino non è crittografato a riposo.

Un punto di AWS Backup ripristino si riferisce a una copia o istantanea specifica dei dati creata come parte di un processo di backup. Rappresenta un momento particolare in cui è stato eseguito il backup dei dati e funge da punto di ripristino nel caso in cui i dati originali vengano persi, danneggiati o inaccessibili. La crittografia dei punti di ripristino del backup aggiunge un ulteriore livello di protezione contro l'accesso non autorizzato. La crittografia è una procedura ottimale per proteggere la riservatezza, l'integrità e la sicurezza dei dati di backup.

Correzione

Per crittografare un punto di AWS Backup ripristino, consulta Encryption for backup AWS Backup nella AWS Backup Developer Guide.

[Backup.2] AWS Backup i punti di ripristino devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Backup::RecoveryPoint`

AWS Config regola: `tagged-backup-recoverypoint` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un punto di AWS Backup ripristino dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il punto di ripristino non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il punto di ripristino non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per copiare i tag dalle risorse di origine al momento della creazione del backup, consulta Copiare i tag sui backup nella AWS Backup Guida per gli sviluppatori.

I tag non vengono copiati al momento della creazione per i punti di parent/composite ripristino. Per aggiungere tag ai punti di ripristino esistenti, inclusi i punti di parent/composite ripristino, consulta Aggiungere o rimuovere tag sui punti di ripristino esistenti nella Guida per AWS Backup gli sviluppatori.

[Backup.3] AWS Backup i vault devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Backup::BackupVault`

AWS Config regola: `tagged-backup-backupvault` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un AWS Backup vault ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il punto di ripristino non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il punto di ripristino non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un AWS Backup vault

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegliere Backup vaults (Vault di backup).
3. Seleziona un archivio di backup dall'elenco.
4. Nella sezione Backup vault tags, scegli Gestisci tag.
5. Immettere una chiave e un valore per il tag. Scegli Aggiungi nuovo tag per ulteriori coppie chiave-valore.
6. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

[Backup.4] AWS Backup i piani di report devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Backup::ReportPlan`

AWS Config regola: `tagged-backup-reportplan` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un piano di AWS Backup report contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il piano di report non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se al piano di report non è associata alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un AWS Backup piano di rapporto

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegliere Backup vaults (Vault di backup).
3. Seleziona un archivio di backup dall'elenco.
4. Nella sezione Backup vault tags, scegli Gestisci tag.
5. Scegli Aggiungi nuovo tag. Immettere una chiave e un valore per il tag. Ripetere l'operazione per ulteriori coppie chiave-valore.
6. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

[Backup.5] AWS Backup i piani di backup devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Backup::BackupPlan`

AWS Config regola: `tagged-backup-backupplan` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un piano AWS Backup di backup dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il piano di backup non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il piano di backup non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un AWS Backup piano di backup

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegliere Backup vaults (Vault di backup).
3. Seleziona un archivio di backup dall'elenco.
4. Nella sezione Backup vault tags, scegli Gestisci tag.
5. Scegli Aggiungi nuovo tag. Immettere una chiave e un valore per il tag. Ripetere l'operazione per ulteriori coppie chiave-valore.
6. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

Controlli CSPM Security Hub per AWS Batch

Questi controlli CSPM di Security Hub valutano il AWS Batch servizio e le risorse. I controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Batch.1] Le code di lavoro in batch devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Batch::JobQueue`

Regola AWS Config : batch-job-queue-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfan	Nessun valore predefinito

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	I tag fanno distinzione tra maiuscole e minuscole		o i requisiti AWS .	

Questo controllo verifica se una coda di AWS Batch lavori ha tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se la coda dei processi non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredKeyTags` Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la coda dei processi non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a una coda di lavori Batch, consulta Etichettare le risorse nella Guida per l'AWS Batch utente.

[Batch.2] Le politiche di pianificazione dei batch devono essere etichettate

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Batch::SchedulingPolicy`

Regola AWS Config : batch-scheduling-policy-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se una politica AWS Batch di pianificazione ha tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se la politica di pianificazione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredKeyTags` Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la politica di pianificazione non è contrassegnata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a una politica di pianificazione Batch, consulta Etichettare le risorse nella Guida per l'AWS Batch utente.

[Batch.3] Gli ambienti di calcolo in batch devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Batch::ComputeEnvironment`

Regola AWS Config : batch-compute-environment-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un ambiente di AWS Batch calcolo dispone di tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se l'ambiente di calcolo non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredKeyTags` Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'ambiente di calcolo non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un ambiente di calcolo Batch, consulta Etichettare le risorse nella Guida per l'AWS Batch utente.

[Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Batch::ComputeEnvironment`

Regola AWS Config : batch-managed-compute-env-compute-resources-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se la proprietà delle risorse di calcolo in un ambiente di AWS Batch calcolo gestito ha le chiavi dei tag specificate dal parametro. `requiredKeyTags` Il controllo ha esito negativo se la proprietà compute resources non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal parametro. `requiredKeyTags` Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave tag e fallisce se una proprietà delle risorse di calcolo non dispone di chiavi tag. Il controllo ignora i tag di sistema, che

vengono applicati automaticamente e hanno il `aws:` prefisso. Questo controllo non valuta gli ambienti di elaborazione non gestiti o gli ambienti gestiti che utilizzano risorse. AWS Fargate

Un tag è un'etichetta che crei e assegni a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag alle risorse di calcolo in un ambiente di AWS Batch elaborazione gestito, consulta Etichettare le risorse nella Guida per l'AWS Batch utente.

Controlli CSPM del Security Hub per Amazon Bedrock

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon Bedrock. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Bedrock.1] Le fonti di dati Amazon Bedrock devono essere crittografate e gestite dai clienti AWS KMS keys

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: `AWS::Bedrock::DataSource`

Regola AWS Config : bedrock-data-source-encryption-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'origine dati Amazon Bedrock è crittografata quando è inattiva con una AWS KMS chiave gestita dal cliente. Il controllo fallisce se l'origine dati non è crittografata con una chiave KMS gestita dal cliente. Il controllo non valuta le fonti di dati che appartengono a una knowledge base gestita.

Per impostazione predefinita, Amazon Bedrock crittografa i contenuti delle sorgenti dati con chiavi AWS gestite. L'utilizzo di una chiave KMS gestita dal cliente ti offre il pieno controllo sul ciclo di vita della chiave di crittografia, inclusa la rotazione, le politiche di accesso e il controllo. AWS CloudTrail Questo aiuta a soddisfare i requisiti di conformità che impongono la crittografia controllata dal cliente per i dati sensibili inseriti nelle knowledge base.

Correzione

Per crittografare la tua origine dati Amazon Bedrock con una chiave KMS gestita dal cliente, consulta Modificare un'origine dati per la tua knowledge base Amazon Bedrock nella Amazon Bedrock User Guide.

Controlli CSPM del Security Hub per Amazon Bedrock AgentCore

Questi AWS Security Hub CSPM controlli valutano il AgentCore servizio e le risorse Amazon Bedrock. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC

Categoria: Protezione > Gestione sicura degli accessi > Risorsa non accessibile al pubblico

Gravità: alta

Tipo di risorsa: `AWS::BedrockAgentCore::Runtime`

Regola AWS Config : bedrockagentcore-runtime-private-network-required

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AgentCore runtime Amazon Bedrock è configurato con la modalità di rete VPC. Il controllo fallisce se la modalità di rete del runtime è impostata su PUBLIC.

Il controllo non produce risultati per i runtime supportati da un provider di capacità. Questi runtime definiscono la configurazione di rete sul provider di capacità anziché sul runtime, quindi non rientrano nell'ambito di questo controllo.

L'utilizzo della modalità di rete pubblica per i AgentCore runtime di Amazon Bedrock espone il runtime direttamente a Internet, aumentando la superficie di attacco e il rischio di accessi non autorizzati. La configurazione dei runtime con la modalità di rete VPC garantisce che il traffico di runtime sia limitato all'interno della rete privata, consentendoti di applicare controlli di sicurezza a livello di rete come gruppi di sicurezza, ACL di rete e log di flusso VPC.

Correzione

Per correggere questo problema, aggiorna il AgentCore runtime di Bedrock non conforme e configuralo con la modalità di rete VPC. Per istruzioni, consulta Configurare Amazon Bedrock AgentCore Runtime e gli strumenti per VPC nella Amazon AgentCore Bedrock Developer Guide.

[BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: alta

Tipo di risorsa: `AWS::BedrockAgentCore::Gateway`

Regola AWS Config : bedrockagentcore-gateway-authorizer-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un Amazon Bedrock AgentCore Gateway richiede l'autorizzazione per le richieste in entrata. Il controllo fallisce se su Bedrock AgentCore Gateway non è configurata l'autorizzazione in entrata.

La configurazione dell'autenticazione sui AgentCore gateway Amazon Bedrock garantisce che solo i client autorizzati possano inviare richieste ai tuoi agenti AI. Senza un'autorizzazione, qualsiasi entità con accesso di rete all'endpoint gateway può invocare i tuoi agenti, con conseguenti possibili accessi

non autorizzati ai dati, abuso di risorse o costi imprevisti. L'autorizzazione in entrata convalida gli utenti che tentano di accedere agli obiettivi tramite il gateway. AgentCore

Correzione

Per configurare l'autorizzazione in entrata per un Amazon Bedrock AgentCore Gateway, consulta Configurare l'autorizzazione in entrata per il gateway nella Amazon AgentCore Bedrock Developer Guide.

[BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys

Requisiti correlati: 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)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: `AWS::BedrockAgentCore::Memory`

Regola AWS Config : bedrock-agentcore-memory-encryption-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una AgentCore memoria Amazon Bedrock è crittografata quando è inattiva con una AWS KMS chiave gestita dal cliente. Il controllo fallisce se la Bedrock AgentCore Memory non è crittografata con una chiave KMS gestita dal cliente.

L'utilizzo di una chiave KMS gestita dal cliente per la crittografia della AgentCore memoria Amazon Bedrock offre una maggiore sicurezza rispetto alla chiave gestita dal servizio predefinita. Le chiavi KMS gestite dal cliente offrono il pieno controllo sul ciclo di vita delle chiavi di crittografia e sulle politiche di accesso. Inoltre, tutto l'utilizzo delle chiavi di crittografia può essere registrato e monitorato per verificarne la verificabilità. AWS CloudTrail

Correzione

Per crittografare la tua AgentCore memoria Amazon Bedrock con una chiave KMS gestita dal cliente, consulta Encrypt your Amazon Bedrock AgentCore Memory nella Amazon Bedrock Developer Guide. AgentCore

[BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys

Requisiti correlati: 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)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: `AWS::BedrockAgentCore::Gateway`

Regola AWS Config : bedrockagentcore-gateway-encryption-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un Amazon Bedrock AgentCore Gateway è crittografato quando è inattivo con una AWS KMS chiave gestita dal cliente. Il controllo fallisce se Bedrock AgentCore Gateway non è crittografato con una chiave KMS gestita dal cliente. Il controllo non valuta se la chiave KMS configurata gestita dal cliente è disabilitata o eliminata.

Per impostazione predefinita, Amazon Bedrock AgentCore crittografa i dati del gateway con chiavi AWS gestite. L'utilizzo di una chiave KMS gestita dal cliente ti offre il pieno controllo sul ciclo di vita della chiave di crittografia, inclusa la rotazione, le politiche di accesso e il controllo. AWS CloudTrail Questo aiuta a soddisfare i requisiti di conformità che impongono la crittografia controllata dal cliente per carichi di lavoro di intelligenza artificiale sensibili.

Correzione

Per crittografare il tuo Bedrock AgentCore Gateway con una chiave KMS gestita dal cliente, consulta Crittografa il tuo AgentCore gateway con una chiave KMS gestita dal cliente nella Amazon Bedrock Developer Guide. AgentCore

[BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Gravità: alta

Tipo di risorsa: `AWS::BedrockAgentCore::BrowserCustom`

Regola AWS Config : bedrockagentcore-browsercustom-network-mode-not-public

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un browser AgentCore personalizzato Amazon Bedrock è configurato con la modalità di rete pubblica. Il controllo fallisce se la modalità di rete è impostata su pubblica.

L'utilizzo della modalità di rete PUBBLICA per i browser AgentCore personalizzati Amazon Bedrock espone le sessioni del browser direttamente a Internet, aumentando la superficie di attacco e il rischio di accessi non autorizzati. La configurazione dei browser con la modalità di rete VPC garantisce che il traffico del browser sia limitato all'interno della rete privata, consentendoti di applicare controlli di sicurezza a livello di rete come gruppi di sicurezza, ACL di rete e log di flusso VPC.

Correzione

Per correggere questo problema, elimina il browser AgentCore personalizzato Bedrock non conforme e ricrealo con la modalità di rete VPC. Per istruzioni, consulta Configurare Amazon Bedrock AgentCore Runtime e gli strumenti per VPC nella Amazon AgentCore Bedrock Developer Guide.

[BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::BedrockAgentCore::BrowserCustom`

Regola AWS Config : bedrockagentcore-browsercustom-recording-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un browser AgentCore personalizzato Amazon Bedrock ha la registrazione della sessione abilitata con una destinazione S3 configurata. Il controllo ha esito negativo se un browser personalizzato non ha la registrazione abilitata o non ha una posizione S3 configurata per l'archiviazione delle registrazioni.

La registrazione delle sessioni per i browser AgentCore personalizzati Bedrock garantisce la piena verificabilità delle interazioni del browser, consentendo il rilevamento di accessi non autorizzati, esfiltrazione di dati o attività dannose durante le sessioni di navigazione automatizzate.

Correzione

Per istruzioni su come abilitare la registrazione delle sessioni del browser, consulta Session Recording and Replay nella Amazon Bedrock AgentCore Developer Guide.

[BedrockAgentCore.7] Gli interpreti di codice AgentCore personalizzato Bedrock devono utilizzare una configurazione di rete privata

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Gravità: alta

Tipo di risorsa: `AWS::BedrockAgentCore::CodeInterpreterCustom`

Regola AWS Config : bedrockagentcore-codeinterpreter-networkmode-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un interprete di codice AgentCore personalizzato Amazon Bedrock è configurato con una modalità di rete privata. Il controllo fallisce se la modalità di rete è impostata su o`PUBLIC`. `SANDBOX`

La configurazione degli interpreti di codice AgentCore personalizzati Bedrock con una modalità di rete privata garantisce che gli ambienti di esecuzione del codice siano isolati all'interno del tuo VPC. Le modalità di rete pubbliche o sandbox espongono l'interprete di codice a Internet, aumentando il rischio di accesso non autorizzato e di esfiltrazione dei dati. L'utilizzo della modalità di rete privata limita l'accesso alla rete e aiuta a proteggere i dati sensibili elaborati durante l'interpretazione del codice.

Correzione

Per correggere questo risultato, elimina l'interprete di codice AgentCore personalizzato Bedrock non conforme e ricrealo con la modalità di rete VPC. Per istruzioni, consulta Configurazione dell'accesso VPC per runtime e strumenti nella Amazon AgentCore Bedrock Developer Guide.

Controlli CSPM Security Hub per AWS Certificate Manager

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse AWS Certificate Manager (ACM). I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato

Requisiti correlati: 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. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06, Profilo CRI v2. 2/PR. PS-01.07

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ACM::Certificate`

Regola AWS Config : acm-certificate-expiration-check

Tipo di pianificazione: modifica attivata e periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`daysToExpiration`	Numero di giorni entro i quali il certificato ACM deve essere rinnovato	Numero intero	Da `14` a `365`	`30`

Questo controllo verifica se un certificato AWS Certificate Manager (ACM) viene rinnovato entro il periodo di tempo specificato. Controlla sia i certificati importati che i certificati forniti da ACM. Il controllo fallisce se il certificato non viene rinnovato entro il periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di rinnovo, Security Hub CSPM utilizza un valore predefinito di 30 giorni.

ACM può rinnovare automaticamente i certificati che utilizzano la convalida DNS. Per i certificati che utilizzano la convalida e-mail, è necessario rispondere a un'e-mail di convalida del dominio. ACM non rinnova automaticamente i certificati importati. È necessario rinnovare manualmente i certificati importati.

Correzione

ACM offre un rinnovo gestito per i tuoi SSL/TLS certificati emessi da Amazon. Ciò significa che ACM rinnova i certificati automaticamente (se utilizzi la convalida DNS) oppure ti invia notifiche via e-mail quando si avvicina la scadenza del certificato. Questi servizi sono forniti sia per i certificati ACM pubblici che privati.

Per i domini convalidati tramite e-mail

Quando mancano 45 giorni alla scadenza di un certificato, ACM invia al proprietario del dominio un'e-mail per ogni nome di dominio. Per convalidare i domini e completare il rinnovo, devi rispondere alle notifiche e-mail.

Per ulteriori informazioni, consulta Rinnovo per domini convalidati tramite e-mail nella Guida per l'utente.AWS Certificate Manager

Per i domini convalidati dal DNS

ACM rinnova automaticamente i certificati che utilizzano la convalida DNS. 60 giorni prima della scadenza, ACM verifica che il certificato possa essere rinnovato.

Se non è in grado di convalidare un nome di dominio, ACM invia una notifica indicante che è necessaria la convalida manuale. Invia queste notifiche 45 giorni, 30 giorni, 7 giorni e 1 giorno prima della scadenza.

Per ulteriori informazioni, consulta Rinnovo per i domini convalidati dal DNS nella Guida per l'AWS Certificate Manager utente.

[ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit

Requisiti correlati: PCI DSS v4.0. 1/4.2.1, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Identificazione > Inventario > Servizi di inventario

Gravità: alta

Tipo di risorsa: `AWS::ACM::Certificate`

Regola AWS Config : acm-certificate-rsa-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i certificati RSA gestiti da AWS Certificate Manager utilizzano una lunghezza di chiave di almeno 2.048 bit. Il controllo ha esito negativo se la lunghezza della chiave è inferiore a 2.048 bit.

La forza della crittografia è direttamente correlata alla dimensione della chiave. Consigliamo una lunghezza delle chiavi di almeno 2.048 bit per proteggere AWS le risorse in quanto la potenza di calcolo diventa meno costosa e i server diventano più avanzati.

Correzione

La lunghezza minima delle chiavi per i certificati RSA emessi da ACM è già di 2.048 bit. Per istruzioni sull'emissione di nuovi certificati RSA con ACM, consulta Emissione e gestione dei certificati nella Guida per l'utente.AWS Certificate Manager

Sebbene ACM consenta di importare certificati con chiavi di lunghezza inferiore, è necessario utilizzare chiavi di almeno 2.048 bit per passare questo controllo. Non è possibile modificare la lunghezza della chiave dopo aver importato un certificato. È invece necessario eliminare i certificati con una lunghezza di chiave inferiore a 2.048 bit. Per ulteriori informazioni sull'importazione di certificati in ACM, consulta Prerequisiti per l'importazione dei certificati nella Guida per l'utente.AWS Certificate Manager

[ACM.3] I certificati ACM devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::ACM::Certificate`

AWS Config regola: `tagged-acm-certificate` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un certificato AWS Certificate Manager (ACM) contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo ha esito negativo se il certificato non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il certificato non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un certificato ACM, consulta Taggare i AWS Certificate Manager certificati nella Guida per l'utente.AWS Certificate Manager

Controlli CSPM Security Hub perCloudFormation

Questi controlli CSPM di Security Hub valutano il AWS CloudFormation servizio e le risorse.

Questi controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[CloudFormation.1] CloudFormation gli stack devono essere integrati con Simple Notification Service (SNS)

> **Important**
>
> Security Hub CSPM ha ritirato questo controllo nell'aprile 2024. Per ulteriori informazioni, consulta Registro delle modifiche per i controlli CSPM di Security Hub.

Requisiti correlati: NIST.800-53.r5 SI-4 (12), (5) NIST.800-53.r5 SI-4

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: `AWS::CloudFormation::Stack`

Regola AWS Config: `cloudformation-stack-notification-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una notifica di Amazon Simple Notification Service è integrata con uno CloudFormation stack. Il controllo fallisce per uno CloudFormation stack se non è associata alcuna notifica SNS.

La configurazione di una notifica SNS con lo CloudFormation stack consente di notificare immediatamente alle parti interessate eventuali eventi o modifiche che si verificano nello stack.

Correzione

Per integrare uno CloudFormation stack e un argomento SNS, consulta Aggiornamento degli stack direttamente nella Guida per l'utente. AWS CloudFormation

[CloudFormation.2] gli CloudFormation stack devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::CloudFormation::Stack`

AWS Configregola: `tagged-cloudformation-stack` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se uno AWS CloudFormation stack ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se lo stack non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se lo stack non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a uno CloudFormation stack, consulta l'AWS CloudFormationAPI CreateStackReference.

[CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata

Categoria: Proteggi > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: media

Tipo di risorsa: `AWS::CloudFormation::Stack`

Regola AWS Config: cloudformation-termination-protection-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se uno AWS CloudFormation stack ha la protezione dalla terminazione abilitata. Il controllo fallisce se la protezione dalla terminazione non è abilitata su uno stack. CloudFormation

CloudFormation aiuta a gestire le risorse correlate come una singola unità denominata Stack. Puoi impedire che uno stack venga eliminato accidentalmente abilitando la protezione da cessazione sullo stack. Se un utente tenta di eliminare uno stack con protezione da cessazione abilitata, l'eliminazione ha esito negativo e lo stack, incluso lo stato, rimane invariato. Puoi impostare la protezione da cessazione su stack con qualsiasi stato eccetto `DELETE_IN_PROGRESS` o `DELETE_COMPLETE`.

> **Note**
>
> Se abilitata o disabilitata su uno stack, la protezione da cessazione approva la stessa scelta anche per qualsiasi stack nidificato appartenente a tale stack. Non è possibile abilitare o disabilitare la protezione da terminazione direttamente su uno stack nidificato. Non è possibile eliminare direttamente uno stack annidato appartenente a uno stack con la protezione dalla terminazione abilitata. Se accanto al nome dello stack compare la dicitura NESTED (NIDIFICATO), si tratta di uno stack nidificato. È possibile modificare la protezione da cessazione soltanto sullo stack radice al quale appartiene lo stack nidificato.

Correzione

Per abilitare la protezione dalla terminazione su uno CloudFormation stack, consulta Proteggere gli CloudFormation stack dall'eliminazione nella Guida per l'utente. AWS CloudFormation

[CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati

Categoria: Rileva > Gestione sicura degli accessi

Gravità: media

Tipo di risorsa: `AWS::CloudFormation::Stack`

Regola AWS Config: cloudformation-stack-service-role-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se a uno AWS CloudFormation stack è associato un ruolo di servizio. Il controllo ha esito negativo per uno CloudFormation stack se non è associato alcun ruolo di servizio.

Service-managed StackSets utilizza i ruoli di esecuzione tramite AWS Organizations trusted access integration. Il controllo genera inoltre un risultato NON RIUSCITO per uno AWS CloudFormation

stack creato da service-managed StackSets perché non vi è alcun ruolo di servizio associato. A causa della modalità di StackSets autenticazione gestita dal servizio, il `roleARN` campo non può essere compilato per questi stack.

L'utilizzo dei ruoli di servizio con CloudFormation gli stack consente di implementare l'accesso con privilegi minimi separando le autorizzazioni tra l'utente che creates/updates si occupa dello stack e le autorizzazioni necessarie alle risorse. CloudFormation create/update Ciò riduce il rischio di aumento dei privilegi e aiuta a mantenere i confini di sicurezza tra i diversi ruoli operativi.

> **Note**
>
> Non è possibile rimuovere un ruolo di servizio collegato a uno stack dopo la creazione dello stack. Altri utenti che dispongono delle autorizzazioni per eseguire operazioni su questo stack potranno usare questo ruolo, indipendentemente dal fatto che dispongano o meno dell'autorizzazione `iam:PassRole`. Se il ruolo include le autorizzazioni di cui l'utente non dovrebbe disporre, puoi riassegnare involontariamente le autorizzazioni di un utente. Assicurati che il ruolo garantisca i privilegi minimi.

Correzione

Per associare un ruolo di servizio a uno CloudFormation stack, consulta il ruolo di CloudFormation servizio nella Guida per l'utente. AWS CloudFormation

Controlli CSPM Security Hub per Amazon CloudFront

Questi AWS Security Hub CSPM controlli valutano il CloudFront servizio e le risorse Amazon. I controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato

Requisiti correlati: NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), PCI DSS v4.0. 1/2.2.6, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Gestione sicura degli accessi > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-default-root-object-configured

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una CloudFront distribuzione Amazon con origini S3 è configurata per restituire un oggetto specifico che è l'oggetto root predefinito. Il controllo fallisce se la CloudFront distribuzione utilizza origini S3 e non ha un oggetto root predefinito configurato. Questo controllo non si applica alle CloudFront distribuzioni che utilizzano origini personalizzate.

A volte un utente può richiedere l'URL principale della distribuzione anziché un oggetto nella distribuzione. In tal caso, la specifica di un oggetto root predefinito può contribuire a evitare l'esposizione dei contenuti della distribuzione Web.

Correzione

Per configurare un oggetto radice predefinito per una CloudFront distribuzione, consulta Come specificare un oggetto radice predefinito nella Amazon CloudFront Developer Guide.

[CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito

Requisiti correlati: 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), PCI DSS v4.0. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-viewer-policy-https

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una CloudFront distribuzione Amazon richiede agli spettatori di utilizzare direttamente HTTPS o se utilizza il reindirizzamento. Il controllo fallisce se `ViewerProtocolPolicy` è impostato su `allow-all` for `defaultCacheBehavior` o for. `cacheBehaviors`

Puoi utilizzare HTTPS (TLS) per impedire a potenziali aggressori di utilizzare attacchi di tipo person-in-the-middle o simili per intercettare o manipolare traffico di rete. Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS). La crittografia dei dati in transito può influire sulle prestazioni. È consigliabile testare l'applicazione con questa funzionalità per comprendere il profilo delle prestazioni e l'impatto del TLS.

Correzione

Per crittografare una CloudFront distribuzione in transito, consulta la sezione Richiedere HTTPS per la comunicazione tra gli spettatori e CloudFront nella Amazon CloudFront Developer Guide.

[CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: bassa

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-origin-failover-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una CloudFront distribuzione Amazon è configurata con un gruppo di origine che ha due o più origini.

CloudFront il failover di origine può aumentare la disponibilità. Il failover di origine reindirizza automaticamente il traffico verso un'origine secondaria se l'origine principale non è disponibile o se restituisce codici di stato di risposta HTTP specifici.

Correzione

Per configurare il failover di origine per una CloudFront distribuzione, consulta Creating an origin group nella Amazon CloudFront Developer Guide.

[CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata

Requisiti correlati: 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. 1/10.4.2, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-accesslogs-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione degli accessi al server è abilitata sulle CloudFront distribuzioni. Il controllo ha esito negativo se la registrazione dei log di accesso non è abilitata per una distribuzione. Questo controllo valuta solo se la registrazione standard (legacy) è abilitata per una distribuzione.

CloudFront i registri di accesso forniscono informazioni dettagliate su ogni richiesta utente ricevuta. CloudFront Ogni log contiene informazioni come la data e l'ora di ricezione della richiesta, l'indirizzo IP del visualizzatore che ha effettuato la richiesta, l'origine della richiesta e il numero di porta della richiesta del visualizzatore. Questi log sono utili per applicazioni quali audit di sicurezza e accesso e indagini forensi. Per ulteriori informazioni sull'analisi dei log di accesso, consulta Interroga i CloudFront log di Amazon nella Amazon Athena User Guide.

Correzione

Per configurare la registrazione standard (legacy) per una CloudFront distribuzione, consulta Configure standard logging (legacy) nella Amazon CloudFront Developer Guide.

[CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato

Requisiti correlati: NIST.800-53.r5 AC-4 (21), PCI DSS v4.0. 1/6.4.2, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/GV. OC-04.03, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-01.05, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Proteggi > Servizi di protezione

Gravità: media

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-associated-with-waf

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni sono associate agli ACL AWS WAF classici o AWS WAF Web. Il controllo ha esito negativo se la distribuzione non è associata a un ACL web.

AWS WAF è un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web e le API dagli attacchi. Consente di configurare un set di regole denominato lista di controllo degli accessi Web (ACL web) per consentire, bloccare o contare le richieste Web in base a condizioni e regole di sicurezza Web personalizzabili definite dall'utente. Assicurati che la tua CloudFront distribuzione sia associata a un ACL AWS WAF web per proteggerla da attacchi dannosi.

Correzione

Per associare un ACL AWS WAF Web a una CloudFront distribuzione, consulta Using AWS WAF to control access to your content nella Amazon CloudFront Developer Guide.

[CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS

Requisiti correlati: 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, Profilo CRI v2. 2/ PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: bassa

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-custom-ssl-certificate

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni utilizzano i SSL/TLS certificati CloudFront predefiniti forniti. Questo controllo passa se la CloudFront distribuzione utilizza un SSL/TLS certificato

personalizzato. Questo controllo ha esito negativo se la CloudFront distribuzione utilizza il SSL/TLS certificato predefinito.

SSL/TLS Consenti agli utenti di accedere ai contenuti in modo personalizzato utilizzando nomi di dominio alternativi. Puoi archiviare certificati personalizzati in AWS Certificate Manager (consigliato) o in IAM.

Correzione

Per aggiungere un nome di dominio alternativo per una CloudFront distribuzione utilizzando un SSL/TLS certificato personalizzato, consulta Aggiungere un nome di dominio alternativo nella Amazon CloudFront Developer Guide.

[CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Configurazione di rete protetta

Gravità: bassa

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-sni-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni Amazon utilizzano un SSL/TLS certificato personalizzato e sono configurate per utilizzare SNI per soddisfare le richieste HTTPS. Questo controllo fallisce se è associato un SSL/TLS certificato personalizzato ma il metodo di SSL/TLS supporto è un indirizzo IP dedicato. Il controllo fallisce anche se la distribuzione utilizza CloudFront SSL/TLS un certificato predefinito.

Server Name Indication (SNI) è un'estensione del protocollo TLS supportato da browser e client rilasciati dopo il 2010. Se configuri CloudFront per servire le richieste HTTPS utilizzando SNI, CloudFront associa il nome di dominio alternativo a un indirizzo IP per ogni edge location. Quando un visualizzatore invia una richiesta HTTPS per i tuoi contenuti, il DNS instrada la richiesta all'indirizzo IP per la edge location corretta. L'indirizzo IP del nome di dominio viene determinato durante la negoziazione dell' SSL/TLS handshake; l'indirizzo IP non è dedicato alla distribuzione.

Correzione

Per configurare una CloudFront distribuzione per utilizzare SNI per soddisfare le richieste HTTPS, consulta Utilizzare SNI per servire le richieste HTTPS (funziona per la maggior parte dei client) nella Guida per gli sviluppatori. CloudFront Per informazioni sui certificati SSL personalizzati, consulta Requisiti per l'utilizzo SSL/TLS dei certificati con. CloudFront

[CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate

Requisiti correlati: 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, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-traffic-to-origin-encrypted

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni Amazon stanno crittografando il traffico verso origini personalizzate. Questo controllo non riesce per una CloudFront distribuzione la cui politica del protocollo di origine consente «solo http». Questo controllo fallisce anche se la politica del protocollo di origine della distribuzione è «match-viewer» mentre la politica del protocollo del visualizzatore è «allow-all».

HTTPS (TLS) può essere utilizzato per impedire l'intercettazione o la manipolazione del traffico di rete. Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS).

Correzione

Per aggiornare la politica del protocollo di origine per richiedere la crittografia per una CloudFront connessione, consulta Richiedere HTTPS per la comunicazione tra CloudFront e la tua origine personalizzata nella Amazon CloudFront Developer Guide.

[CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate

Requisiti correlati: 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),, (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, Profilo CRI v2. 2/PR. PS-01.05, Profilo CRI v2. 2/PR. PS-01.06, Profilo CRI v2. 2/PR. PS-02.03

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-no-deprecated-ssl-protocols

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni Amazon utilizzano protocolli SSL obsoleti per la comunicazione HTTPS tra le CloudFront edge location e le tue origini personalizzate. Questo controllo fallisce se una CloudFront distribuzione include un where include. `CustomOriginConfig` `OriginSslProtocols` `SSLv3`

Nel 2015, l'Internet Engineering Task Force (IETF) ha annunciato ufficialmente che SSL 3.0 dovrebbe essere obsoleto a causa della scarsa sicurezza del protocollo. Si consiglia di utilizzare TLSv1.2 o versioni successive per la comunicazione HTTPS con le origini personalizzate.

Correzione

Per aggiornare i protocolli SSL di origine per una CloudFront distribuzione, consulta Richiedere HTTPS per la comunicazione tra CloudFront e la tua origine personalizzata nella Amazon CloudFront Developer Guide.

[CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti

Requisiti correlati: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), PCI DSS v4.0. 1/22.2.6, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Identificazione > Configurazione delle risorse

Gravità: alta

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-s3-origin-non-existent-bucket

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni Amazon puntano a origini Amazon S3 inesistenti. Il controllo fallisce per una CloudFront distribuzione se l'origine è configurata in modo da puntare a un bucket inesistente. Questo controllo si applica solo alle CloudFront distribuzioni in cui un bucket S3 senza hosting di siti Web statici è l'origine di S3.

Quando una CloudFront distribuzione nel tuo account è configurata in modo che punti a un bucket inesistente, una terza parte malintenzionata può creare il bucket di riferimento e pubblicare i propri contenuti tramite la tua distribuzione. Ti consigliamo di controllare tutte le origini indipendentemente dal comportamento di routing per assicurarti che le distribuzioni puntino alle origini appropriate.

Correzione

Per modificare una CloudFront distribuzione in modo che punti a una nuova origine, consulta la sezione Aggiornamento di una distribuzione nell'Amazon CloudFront Developer Guide.

[CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine

Requisiti correlati: CRI Profile v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-03.02

Categoria: Protezione > Gestione sicura degli accessi > Risorsa non accessibile al pubblico

Gravità: media

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-s3-origin-access-control-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una CloudFront distribuzione Amazon con un'origine Amazon S3 ha configurato il controllo dell'accesso all'origine (OAC). Il controllo fallisce se OAC non è configurato per la distribuzione. CloudFront

Quando usi un bucket S3 come origine per la tua CloudFront distribuzione, puoi abilitare OAC. Ciò consente l'accesso al contenuto del bucket solo tramite la CloudFront distribuzione specificata e proibisce l'accesso diretto dal bucket o da un'altra distribuzione. Sebbene CloudFront supporti Origin Access Identity (OAI), OAC offre funzionalità aggiuntive e le distribuzioni che utilizzano OAI possono migrare verso OAC. Sebbene OAI fornisca un modo sicuro per accedere alle origini di S3, presenta delle limitazioni, come la mancanza di supporto per le configurazioni granulari delle policy e per le HTTP/HTTPS richieste che utilizzano il metodo POST e che richiedono la versione 4 della firma (SigV4). Regioni AWS AWS OAI inoltre non supporta la crittografia con. AWS Key Management Service OAC si basa su una AWS best practice di utilizzo dei principali di servizio IAM per l'autenticazione con le origini S3.

Correzione

Per configurare OAC per una CloudFront distribuzione con origini S3, consulta Restricting access to an Amazon S3 origin nella Amazon Developer Guide. CloudFront

[CloudFront.14] CloudFront le distribuzioni devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::CloudFront::Distribution`

AWS Config regola: `tagged-cloudfront-distribution` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	I tag fanno distinzione tra maiuscole e minuscole			

Questo controllo verifica se una CloudFront distribuzione Amazon ha tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se la distribuzione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la distribuzione non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una CloudFront distribuzione, consulta Tagging Amazon CloudFront distribution nella Amazon CloudFront Developer Guide.

[CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata

Requisiti correlati: CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-ssl-policy-check

Tipo di pianificazione: modifica attivata

Parametri:`securityPolicies`: `TLSv1.2_2021,TLSv1.2_2025,TLSv1.3_2025` (non personalizzabile)

Questo controllo verifica se una CloudFront distribuzione Amazon è configurata per utilizzare una politica di sicurezza TLS consigliata. Il controllo fallisce se la CloudFront distribuzione non è configurata per utilizzare una politica di sicurezza TLS consigliata.

Se configuri una CloudFront distribuzione Amazon per richiedere agli utenti di utilizzare HTTPS per accedere ai contenuti, devi scegliere una politica di sicurezza e specificare la versione minima del SSL/TLS protocollo da utilizzare. Ciò determina la versione del protocollo CloudFront utilizzata per comunicare con gli spettatori e i codici CloudFront utilizzati per crittografare le comunicazioni. Si consiglia di utilizzare la politica di sicurezza più recente fornita. CloudFront Ciò garantisce che CloudFront utilizzi le suite di crittografia più recenti per crittografare i dati in transito tra un visualizzatore e una distribuzione. CloudFront

> **Note**
>
> Questo controllo genera risultati solo per CloudFront le distribuzioni configurate per utilizzare certificati SSL personalizzati e non sono configurate per supportare client legacy.

Correzione

Per informazioni sulla configurazione della politica di sicurezza per una CloudFront distribuzione, consulta Aggiornare una distribuzione nella Amazon CloudFront Developer Guide. Quando configuri la politica di sicurezza per una distribuzione, scegli la politica di sicurezza più recente.

[CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Gravità: media

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-origin-lambda-url-oac-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una CloudFront distribuzione Amazon con un URL di AWS Lambda funzione come origine ha il controllo dell'accesso all'origine (OAC) abilitato. Il controllo fallisce se la CloudFront distribuzione ha un URL della funzione Lambda come origine e l'OAC non è abilitato.

L'URL di una AWS Lambda funzione è un endpoint HTTPS dedicato per una funzione Lambda. Se l'URL di una funzione Lambda è l'origine di una CloudFront distribuzione, l'URL della funzione deve essere accessibile pubblicamente. Pertanto, come best practice di sicurezza, è necessario creare un OAC e aggiungerlo all'URL della funzione Lambda in una distribuzione. OAC utilizza i principali del servizio IAM per autenticare le richieste tra CloudFront e l'URL della funzione. Supporta inoltre l'uso di politiche basate sulle risorse per consentire l'invocazione di una funzione solo se una richiesta è per conto di una distribuzione specificata nella policy. CloudFront

Correzione

Per informazioni sulla configurazione di OAC per una CloudFront distribuzione Amazon che utilizza l'URL di una funzione Lambda come origine, consulta Restrict access to an AWS Lambda function URL origin nella Amazon Developer Guide. CloudFront

[CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Gravità: media

Tipo di risorsa: `AWS::CloudFront::Distribution`

Regola AWS Config : cloudfront-distribution-key-group-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una CloudFront distribuzione Amazon è configurata per utilizzare gruppi di chiavi affidabili per l'autenticazione di URL firmati o cookie firmati. Il controllo fallisce se la CloudFront distribuzione utilizza firmatari attendibili o se non è configurata alcuna autenticazione.

Per utilizzare URL firmati o cookie firmati, hai bisogno di un firmatario. Un firmatario è un gruppo di chiavi attendibile in cui CloudFront crei o un AWS account che contiene una coppia di CloudFront chiavi. Ti consigliamo di utilizzare gruppi di chiavi affidabili perché con i gruppi di CloudFront chiavi non è necessario utilizzare l'utente root dell' AWS account per gestire le chiavi pubbliche degli URL CloudFront firmati e dei cookie firmati.

> **Note**
>
> Questo controllo non valuta le distribuzioni multi-tenant CloudFront . `(connectionMode=tenant-only)`

Correzione

Per informazioni sull'utilizzo di gruppi di chiavi affidabili con URL e cookie firmati, consulta Using trusted key groups nella Amazon CloudFront Developer Guide.

Controlli CSPM Security Hub per AWS CloudTrail

Questi AWS Security Hub CSPM controlli valutano il AWS CloudTrail servizio e le risorse. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/3.1, benchmark AWS CIS Foundations v1.2. 0/2.1, benchmark AWS CIS Foundations v1.4. 0/3.1, benchmark AWS CIS 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-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-14 (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 SA-8

(22), NIST.800-53.r5 SI-7 profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: alta

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : multi-region-cloudtrail-enabled

Tipo di pianificazione: periodica

Parametri:

- `readWriteType`: `ALL` (non personalizzabile)

  `includeManagementEvents`: `true` (non personalizzabile)

Questo controllo verifica se esiste almeno un AWS CloudTrail percorso multiregionale che acquisisce gli eventi di gestione di lettura e scrittura. Il controllo fallisce se CloudTrail è disabilitato o se non esiste almeno una CloudTrail traccia che acquisisca gli eventi di gestione di lettura e scrittura.

AWS CloudTrail registra le chiamate AWS API per il tuo account e ti invia i file di registro. Le informazioni registrate includono le seguenti informazioni:

- Identità del chiamante API
- Ora della chiamata API
- Indirizzo IP di origine del chiamante API
- Parametri della richiesta
- Elementi di risposta restituiti da Servizio AWS

CloudTrail fornisce una cronologia delle chiamate AWS API per un account, incluse le chiamate API effettuate dagli Console di gestione AWS strumenti a riga di comando AWS SDK. La cronologia include anche le chiamate API di livello superiore Servizi AWS come. AWS CloudFormation

La cronologia delle chiamate AWS API prodotta da CloudTrail consente l'analisi della sicurezza, il monitoraggio delle modifiche alle risorse e il controllo della conformità. Multi-Region i trail offrono anche i seguenti vantaggi.

- Un trail basato su più regioni aiuta a rilevare le attività impreviste che si verificano in regioni altrimenti inutilizzate.
- Un trail basato su più regioni garantisce che la registrazione dei servizi globali sia abilitata per un trail per impostazione predefinita. La registrazione degli eventi di servizio globale registra gli eventi generati dai servizi AWS globali.
- Per un percorso multiregionale, gli eventi di gestione per tutte le operazioni di lettura e scrittura assicurano che le operazioni di gestione dei CloudTrail record su tutte le risorse in un unico file. Account AWS

Per impostazione predefinita, i CloudTrail percorsi creati utilizzando i percorsi Console di gestione AWS sono multiregionali.

Correzione

Per creare un nuovo percorso multiregionale in CloudTrail, vedi Creazione di un percorso nella Guida per l'AWS CloudTrail utente. Utilizzare i seguenti valori:

Campo	Valore
Impostazioni aggiuntive, Convalida del file di registro	Abilitato
Scegli gli eventi di registro, gli eventi di gestione, l'attività delle API	Leggi e scrivi. Deseleziona le caselle di controllo per le esclusioni.

Per aggiornare un percorso esistente, vedi Aggiornamento di un percorso nella Guida per l'AWS CloudTrail utente. In Management events, per l'attività dell'API, scegli Leggi e scrivi.

[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/3.5, benchmark AWS CIS Foundations v1.2. 0/2.7, benchmark AWS CIS Foundations v1.4. 0/3.7, benchmark AWS CIS Foundations v3.0. 0/3.5, NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 AU-9, (6),, NIST.800-53.r5 CM-3 (1) NIST.800-53.r5 SC-13, (10) NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (6), NIST.800-53.r5 SC-7 NIST.800-171.r2 3.3.8, NIST.800-53.r5 SI-7 PCI DSS versione 3.2. 1/3.4, PCI DSS versione 4.0. 1/10.3.2, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::CloudTrail::Trail`

Regola AWS Config : cloud-trail-encryption-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se CloudTrail è configurato per utilizzare la crittografia lato server (SSE). AWS KMS key Il controllo ha esito negativo se non `KmsKeyId` è definito.

Per un ulteriore livello di sicurezza per i file di CloudTrail registro sensibili, è consigliabile utilizzare la crittografia lato server con AWS KMS keys (SSE-KMS) per la crittografia dei file di CloudTrail registro inattivi. Tieni presente che, per impostazione predefinita, i file di registro forniti dai CloudTrail tuoi bucket sono crittografati mediante crittografia lato server di Amazon con chiavi di S3-managed crittografia Amazon (). SSE-S3

Correzione

Per abilitare SSE-KMS la crittografia per i file di CloudTrail registro, consulta Aggiornare un percorso per utilizzare una chiave KMS nella Guida per l'utente.AWS CloudTrail

[CloudTrail.3] Almeno un CloudTrail percorso deve essere abilitato

Requisiti correlati: 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. 1/10.1, PCI DSS versione 3.2. 1/10.2.1, PCI DSS versione 3.2. 1/10.2.2, PCI DSS versione 3.2. 1/10.2.3, PCI DSS versione 3.2. 1/10.2.4, PCI DSS versione 3.2. 1/10.2.5, PCI DSS versione 3.2. 1/10.2.6, PCI DSS versione 3.2. 1/10.2.7, PCI DSS versione 3.2. 1/10.3.1, PCI DSS versione 3.2. 1/10.3.2, PCI DSS versione 3.2. 1/10.3.3, PCI DSS versione 3.2. 1/10.3.4, PCI DSS versione 3.2. 1/10.3.5, PCI DSS versione 3.2. 1/10.3.6, PCI DSS versione 4.0. 1/10.2.1, Profilo CRI v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01

Categoria: Identificazione > Registrazione

Gravità: alta

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : cloudtrail-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un AWS CloudTrail percorso è abilitato nel tuo Account AWS. Il controllo fallisce se il tuo account non ha almeno un CloudTrail trail abilitato.

Tuttavia, alcuni AWS servizi non consentono la registrazione di tutte le API e gli eventi. È necessario implementare eventuali percorsi di controllo aggiuntivi diversi da quelli indicati nella sezione Servizi CloudTrail e integrazioni CloudTrail supportati e consultare la documentazione relativa a ciascun servizio.

Correzione

Per iniziare CloudTrail e creare un percorso, consulta il AWS CloudTrail tutorial Guida introduttiva nella Guida per l'AWS CloudTrail utente.

[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/3.2, benchmark AWS CIS Foundations v1.2. 0/2.2, benchmark AWS CIS Foundations v1.4. 0/3.2, benchmark AWS CIS Foundations v3.0. 0/3.2, NIST.800-53.r5 AU-9, NIST.800-53.r5 SI-7 (1) NIST.800-53.r5 SI-4, (3), NIST.800-53.r5 SI-7 NIST.800-53.r5 SI-7 (7), NIST.800-171.r2 3.3.8, PCI DSS versione 3.2. 1/105.2, PCI DSS versione 3.2. 1/10.5.5, PCI DSS versione 4.0. 1/10.3.2, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01

Categoria: Protezione dei dati > Integrità dei dati

Gravità: bassa

Tipo di risorsa: `AWS::CloudTrail::Trail`

Regola AWS Config : cloud-trail-log-file-validation-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la convalida dell'integrità dei file di registro è abilitata su una CloudTrail traccia.

CloudTrail la convalida dei file di registro crea un file digest con firma digitale che contiene un hash di ogni log che scrive CloudTrail su Amazon S3. Puoi utilizzare questi file digest per determinare se un file di registro è stato modificato, eliminato o è rimasto invariato dopo la consegna del log. CloudTrail

Security Hub CSPM consiglia di abilitare la convalida dei file su tutti i percorsi. La convalida dei file di registro fornisce ulteriori controlli di integrità dei registri. CloudTrail

Correzione

Per abilitare la convalida dei file di CloudTrail registro, vedere Attivazione della convalida dell'integrità dei file di registro CloudTrail nella Guida per l'utente.AWS CloudTrail

[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/3.4, PCI DSS v3.2. 1/105.3, benchmark CIS Foundations v1.2 AWS . 0/2.4, benchmark AWS CIS 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-3, NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (3), (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) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (20), (5), NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-4 profilo CRI NIST.800-53.r5 SI-7 v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::CloudTrail::Trail`

Regola AWS Config : cloud-trail-cloud-watch-logs-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se i CloudTrail trail sono configurati per inviare log a CloudWatch Logs. Il controllo fallisce se la `CloudWatchLogsLogGroupArn` proprietà del percorso è vuota.

CloudTrail registra le chiamate AWS API effettuate in un determinato account. Le informazioni registrate includono quanto segue:

- L'identità del chiamante dell'API
- L'ora della chiamata API
- L'indirizzo IP di origine del chiamante API
- I parametri della richiesta
- Gli elementi di risposta restituiti da Servizio AWS

CloudTrail utilizza Amazon S3 per l'archiviazione e la distribuzione dei file di registro. Puoi acquisire CloudTrail i log in un bucket S3 specificato per analisi a lungo termine. Per eseguire analisi in tempo reale, puoi configurare l'invio dei log CloudTrail a Logs. CloudWatch

Per un percorso abilitato in tutte le regioni di un account, CloudTrail invia i file di registro da tutte le regioni a un gruppo di log dei CloudWatch registri.

Security Hub CSPM consiglia di inviare i log a CloudTrail Logs. CloudWatch Tieni presente che questa raccomandazione ha lo scopo di garantire che l'attività dell'account venga rilevata, monitorata e attivata in modo appropriato. Puoi usare CloudWatch Logs per configurarlo con il tuo. Servizi AWS Questa raccomandazione non preclude l'uso di una soluzione diversa.

L'invio di CloudTrail log a CloudWatch Logs facilita la registrazione storica e in tempo reale delle attività in base a utente, API, risorsa e indirizzo IP. È possibile utilizzare questo approccio per stabilire allarmi e notifiche per attività anomale o riservate dell'account.

Correzione

Per l'integrazione CloudTrail con CloudWatch i registri, consulta Invio di eventi ai CloudWatch registri nella Guida per l'utente.AWS CloudTrail

[CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/2.3, benchmark AWS CIS Foundations v1.4. 0/3.3, PCI DSS versione 4.0. 1/1.4.4, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01

Categoria: Identificazione > Registrazione

Severità: critica

Tipo di risorsa: `AWS::S3::Bucket`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica e con attivazione di modifiche

Parametri: nessuno

CloudTrail registra un record di ogni chiamata API effettuata nel tuo account. Questi file di log sono archiviati in un bucket S3. Il CIS consiglia di applicare la policy del bucket S3, o lista di controllo degli accessi (ACL), al bucket S3 che CloudTrail registra per impedire l'accesso pubblico ai log. CloudTrail Consentire l'accesso pubblico ai contenuti dei CloudTrail log potrebbe aiutare un avversario a identificare i punti deboli nell'uso o nella configurazione dell'account interessato.

Per eseguire questo controllo, Security Hub CSPM utilizza innanzitutto una logica personalizzata per cercare il bucket S3 in cui sono archiviati i CloudTrail log. Utilizza quindi le regole AWS Config gestite per verificare che il bucket sia accessibile pubblicamente.

Se aggregate i log in un unico bucket S3 centralizzato, Security Hub CSPM esegue il controllo solo rispetto all'account e alla regione in cui si trova il bucket S3 centralizzato. Per altri account e regioni, lo stato del controllo è Nessun dato.

Se il bucket è accessibile pubblicamente, il controllo genera un risultato non riuscito.

Correzione

Per bloccare l'accesso pubblico al tuo bucket CloudTrail S3, consulta Configurazione delle impostazioni di blocco dell'accesso pubblico per i tuoi bucket S3 nella Guida per l'utente di Amazon Simple Storage Service. Seleziona tutte e quattro le impostazioni di accesso pubblico a blocchi di Amazon S3.

[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/2.6, benchmark AWS CIS Foundations v1.4. 0/3.6, benchmark AWS CIS Foundations v3.0. 0/3.4, PCI DSS versione 4.0. 1/10.2.1, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/PR. PS-04.02

Categoria: Identificazione > Registrazione

Gravità: bassa

Tipo di risorsa: `AWS::S3::Bucket`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

La registrazione degli accessi al bucket S3 genera un registro che contiene i record di accesso per ogni richiesta effettuata al bucket S3. Un record dei log di accesso contiene dettagli sulla richiesta, ad esempio il tipo di richiesta, le risorse specificate nella richiesta e l'ora e la data di elaborazione della richiesta.

Il CIS consiglia di abilitare la registrazione degli accessi ai bucket sul bucket S3. CloudTrail

L'abilitazione della registrazione di bucket S3 su bucket S3 di destinazione consente di acquisire tutti gli eventi che potrebbero influenzare gli oggetti in un bucket di destinazione. La configurazione dei log da inserire in un bucket separato consente l'accesso alle informazioni di log, che possono essere utili nei flussi di lavoro di risposta a sicurezza ed errori.

Per eseguire questo controllo, Security Hub CSPM utilizza innanzitutto la logica personalizzata per cercare il bucket in cui sono archiviati CloudTrail i log e quindi utilizza la regola AWS Config gestita per verificare se la registrazione è abilitata.

Se CloudTrail invia file di log da più bucket Amazon S3 Account AWS in un unico bucket Amazon S3 di destinazione, Security Hub CSPM valuta questo controllo solo rispetto al bucket di destinazione nella regione in cui si trova. Questo semplifica le tue scoperte. Tuttavia, dovresti attivare CloudTrail tutti gli account che inviano i log al bucket di destinazione. Per tutti gli account tranne quello che contiene il bucket di destinazione, lo stato del controllo è Nessun dato.

Correzione

Per abilitare la registrazione dell'accesso al server per il tuo bucket CloudTrail S3, consulta Enabling Amazon S3 server access logging nella Amazon Simple Storage Service User Guide.

[] CloudTrail.9 i trail devono essere etichettati CloudTrail

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::CloudTrail::Trail`

AWS Config regola: `tagged-cloudtrail-trail` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un AWS CloudTrail percorso contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il percorso non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il percorso non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un CloudTrail percorso, consulta la sezione AWS CloudTrail API AddTagsReference.

[CloudTrail.10] I data store di eventi di CloudTrail Lake devono essere crittografati con Customer Managed AWS KMS keys

Requisiti correlati: 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)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::CloudTrail::EventDataStore`

Regola AWS Config : event-data-store-cmk-encryption-enabled

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`kmsKeyArns`	Un elenco di Amazon Resource Names (ARN) AWS KMS keys da includere nella valutazione. Il controllo genera un	StringList (massimo 3 articoli)	1—3 ARN di chiavi KMS esistenti. Ad esempio: `arn:aws:kms:us-west-2:111122223333:k`	Nessun valore predefinito

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	`FAILED` risultato se un archivio dati di eventi non è crittografato con una chiave KMS nell'elenco.		`ey/1234abcd-12ab-34cd-56ef-1234567890ab` .	

Questo controllo verifica se un data store di eventi AWS CloudTrail Lake è crittografato quando è inattivo e gestito da un cliente. AWS KMS key Il controllo fallisce se l'archivio dati degli eventi non è crittografato con una chiave KMS gestita dal cliente. Facoltativamente, puoi specificare un elenco di chiavi KMS per il controllo da includere nella valutazione.

Per impostazione predefinita, AWS CloudTrail Lake crittografa gli archivi di dati di eventi con chiavi gestite di Amazon S3 SSE-S3 (), utilizzando AES-256 un algoritmo. Per un controllo aggiuntivo, puoi invece configurare CloudTrail Lake per crittografare un data store di eventi con un customer managed AWS KMS key ()SSE-KMS. Una chiave KMS gestita dal cliente è una chiave AWS KMS key che puoi creare, possedere e gestire in tuo. Account AWS Hai il pieno controllo su questo tipo di chiave KMS. Ciò include la definizione e il mantenimento della politica chiave, la gestione delle sovvenzioni, la rotazione del materiale crittografico, l'assegnazione di tag, la creazione di alias e l'attivazione e la disabilitazione della chiave. È possibile utilizzare una chiave KMS gestita dal cliente nelle operazioni crittografiche per i dati e verificarne l'utilizzo con i log. CloudTrail CloudTrail

Correzione

Per informazioni sulla crittografia di un data store di eventi AWS CloudTrail Lake con un AWS KMS key valore specificato, consulta Update an event data store nella Guida per l'utente.AWS CloudTrail Dopo aver associato un datastore di eventi a una chiave KMS, la chiave KMS non potrà essere rimossa o modificata.

Controlli CSPM Security Hub per Amazon CloudWatch

Questi AWS Security Hub CSPM controlli valutano il CloudWatch servizio e le risorse Amazon. I controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/1.1, benchmark AWS CIS Foundations v1.2. 0/3.3, benchmark AWS CIS Foundations v1.4. 0/1.7, benchmark AWS CIS Foundations v1.4. 0/4.3, NIST.800-171.r2 3.14.6, 3.14.7, PCI DSS versione 3.2. NIST.800-171.r2 1/7.2.1, Profilo CRI v2. 2/DE. AE-02.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-05.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

L'utente root ha accesso illimitato a tutti i servizi e le risorse in un file. Account AWS Si consiglia vivamente di evitare di utilizzare l'utente root per le attività quotidiane. La riduzione al minimo dell'uso dell'utente root e l'adozione del principio del privilegio minimo per la gestione degli accessi riducono il rischio di modifiche accidentali e di divulgazione involontaria di credenziali altamente privilegiate.

Come procedura ottimale, è consigliabile utilizzare le credenziali dell'utente root solo quando necessario per eseguire attività di gestione degli account e dei servizi. Applica le policy AWS Identity and Access Management (IAM) direttamente ai gruppi e ai ruoli ma non agli utenti. Per un tutorial su come configurare un amministratore per l'uso quotidiano, consulta Creazione del primo utente e gruppo di amministratori IAM nella Guida per l'utente IAM

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire i passaggi di controllo esatti prescritti per il controllo 1.7 nel CIS Foundations Benchmark v1.4.0 AWS. Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
Il controllo dà luogo a `FAILED` risultati nei seguenti casi:

- Non è configurato alcun percorso.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.

  Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**
Valore predefinito	**`0`**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *`your-metric-name`* è...	Greater/Equal

Campo	Valore
rispetto a...	**1**

[CloudWatch.2] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.1, NIST.800-171.r2 3.13.1, 3.14.6, NIST.800-171.r2 3.14.7, Profilo CRI v2. NIST.800-171.r2 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per le chiamate API non autorizzate. Il monitoraggio delle chiamate API non autorizzate consente di rilevare errori dell'applicazione e ridurre il tempo necessario per individuare attività malevola.

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 3.1 nel AWS CIS Foundations Benchmark v1.2. Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
Il controllo dà luogo a `FAILED` risultati nei seguenti casi:

- Non è configurato alcun percorso.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.

  Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**
Valore predefinito	**`0`**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *`your-metric-name`* è...	Greater/Equal
rispetto a...	**`1`**

[CloudWatch.3] Assicurati che esistano un filtro metrico di registro e un allarme per l'accesso alla console di gestione senza MFA

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.2, Profilo CRI v2. 2/DE. AE-02.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e accessi alla console di allarme non protetti da MFA. Il monitoraggio per accessi alla console a singolo fattore incrementa la visibilità negli account che non sono protetti da MFA.

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 3.2 nel AWS CIS Foundations Benchmark v1.2. Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

> **Note**
>
> Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
> Il controllo dà luogo a `FAILED` risultati nei seguenti casi:
>
> - Non è configurato alcun percorso.

- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.

  Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**
Valore predefinito	**`0`**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *`your-metric-name`* è...	Greater/Equal
rispetto a...	**`1`**

[CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.4, benchmark AWS CIS Foundations v1.4. 0/4.4, NIST.800-171.r2 3.14.6, 3.14.7, Profilo CRI v2. NIST.800-171.r2 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/PR. PS-01.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se monitorate le chiamate API in tempo reale indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche apportate alle policy IAM. Il monitoraggio di queste modifiche garantisce che i controlli di autenticazione e autorizzazione rimangano invariati.

> **Note**
>
> Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
>
> Il controllo dà luogo a `FAILED` risultati nei seguenti casi:
>
> - Non è configurato alcun percorso.
> - I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.

  Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Note

Il modello di filtro consigliato in queste fasi di riparazione è diverso dal modello di filtro nella guida CIS. I nostri filtri consigliati hanno come target solo gli eventi provenienti dalle chiamate API IAM.

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRolePolicy) || ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) || ($.eventName=DeletePolicy) \|\| ($.eventName=CreatePolicyVersion) || ($.eventName=DeletePolicyVersion) \|\| ($.eventName=AttachRolePolicy) || ($.eventName=DetachRolePolicy) \|\| ($.eventName=AttachUserPolicy) || ($.eventName=DetachUserPolicy) \|\| ($.eventName=AttachGroupPolicy) || ($.eventName=DetachGroupPolicy))}`
Namespace metrico	**`LogMetrics`**

Campo	Valore
Valore del parametro	**1**
Valore predefinito	**0**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *your-metric-name* è...	Greater/Equal
rispetto a...	**1**

[CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrail alla configurazione

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.5, benchmark AWS CIS Foundations v1.4. 0/4.5, NIST.800-171.r2 3.3.8, 3.14.6, 3.14.7, Profilo CRI NIST.800-171.r2 v2. NIST.800-171.r2 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche alle CloudTrail impostazioni di configurazione. Il monitoraggio di queste modifiche garantisce visibilità sostenuta per attività dell'account.

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 4.5 nel CIS Foundations Benchmark AWS v1.4.0. Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

> **Note**
>
> Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
> Il controllo dà luogo a `FAILED` risultati nei seguenti casi:
>
> - Non è configurato alcun percorso.
> - I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.
>
> Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:
>
> - Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
> - Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.
>
>   Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari

organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**

Campo	Valore
Valore predefinito	**0**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *your-metric-name* è...	Greater/Equal
rispetto a...	**1**

[CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per Console di gestione AWS errori di autenticazione

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.6, benchmark AWS CIS Foundations v1.4. 0/4.6, NIST.800-171.r2 3.14.6, 3.14.7, Profilo CRI v2. NIST.800-171.r2 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per i tentativi di autenticazione della console non riusciti. Il monitoraggio degli accessi alla console non riusciti potrebbe ridurre il lead time per rilevare un tentativo di attacco di forza bruta a una credenziale, che potrebbe fornire un indicatore, ad esempio IP di origine, utilizzabile in altre correlazioni eventi.

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire i passaggi di controllo esatti prescritti per il controllo 4.6 nel CIS Foundations Benchmark v1.4.0. AWS Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

> **Note**
>
> Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
> Il controllo dà luogo a `FAILED` risultati nei seguenti casi:
>
> - Non è configurato alcun percorso.
> - I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.
>
> Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:
>
> - Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
> - Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.
>
> Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare

questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**
Valore predefinito	**`0`**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *your-metric-name* è...	Greater/Equal
rispetto a...	**1**

[CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione pianificata delle chiavi gestite dal cliente

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.7, benchmark AWS CIS 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, Profilo CRI v2. NIST.800-171.r2 NIST.800-171.r2 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per le chiavi gestite dal cliente che hanno cambiato lo stato in eliminazione disattivata o pianificata. I dati crittografati con chiavi disabilitate o eliminate non sono più accessibili.

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire i passaggi di controllo esatti prescritti per il controllo 4.7 nel CIS Foundations Benchmark v1.4.0. AWS Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri. Il controllo fallisce anche se contiene. `ExcludeManagementEventSources` `kms.amazonaws.com`

Note

Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
Il controllo dà luogo a `FAILED` risultati nei seguenti casi:

- Non è configurato alcun percorso.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.

  Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**
Valore predefinito	**`0`**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *your-metric-name* è...	Greater/Equal
rispetto a...	**1**

[CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.8, benchmark AWS CIS Foundations v1.4. 0/4.8, NIST.800-171.r2 3.14.6, 3.14.7, Profilo CRI v2. NIST.800-171.r2 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche alle policy dei bucket S3. Il monitoraggio di queste modifiche potrebbe ridurre il tempo necessario per rilevare e correggere policy permissive su bucket S3 sensibili.

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire i passaggi di controllo esatti prescritti per il controllo 4.8 nel CIS Foundations Benchmark v1.4.0. AWS Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

> **Note**
>
> Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
> Il controllo dà luogo a `FAILED` risultati nei seguenti casi:
>
> - Non è configurato alcun percorso.
> - I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.
>
> Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:
>
> - Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
> - Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.
>
>   Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.
>
> Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

`ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
Namespace metrico	**`LogMetrics`**

Campo	Valore
Valore del parametro	**1**
Valore predefinito	**0**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *your-metric-name* è...	Greater/Equal
rispetto a...	**1**

[CloudWatch.9] Assicurati che esistano un filtro metrico di registro e un allarme per AWS Config modifiche alla configurazione

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.9, benchmark AWS CIS Foundations v1.4. 0/4.9, NIST.800-171.r2 3.3.8, 3.14.6, 3.14.7, Profilo CRI NIST.800-171.r2 v2. NIST.800-171.r2 2/DE. CM-09.03, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche alle AWS Config impostazioni di configurazione. Il monitoraggio di queste modifiche garantisce visibilità sostenuta per elementi di configurazione nell'account.

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire i passaggi di controllo esatti prescritti per il controllo 4.9 nel CIS Foundations Benchmark v1.4.0. AWS Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

> **Note**
>
> Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
> Il controllo dà luogo a `FAILED` risultati nei seguenti casi:
>
> - Non è configurato alcun percorso.
> - I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.
>
> Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:
>
> - Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
> - Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.
>
> Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**

Campo	Valore
Valore predefinito	**0**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *your-metric-name* è...	Greater/Equal
rispetto a...	**1**

[CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.10, benchmark AWS CIS Foundations v1.4. 0/4.10, NIST.800-171.r2 3.14.6, 3.14.7, Profilo CRI v2. NIST.800-171.r2 2/DE. AE-02.02, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/DE. CM-01.05, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-01.05, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.02, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti. I gruppi di sicurezza sono un filtro dei pacchetti stateful che controlla il traffico in entrata e in uscita in un VPC.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche ai gruppi di sicurezza. Il monitoraggio di tali modifiche garantisce che le risorse e i servizi non vengano involontariamente esposti.

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire i passaggi di controllo esatti prescritti per il controllo 4.10 nel CIS Foundations Benchmark v1.4.0. AWS Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

> **Note**
>
> Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
> Il controllo dà luogo a `FAILED` risultati nei seguenti casi:
>
> - Non è configurato alcun percorso.
> - I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.
>
> Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:
>
> - Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
> - Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.
>
>   Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM

genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) ||`

Campo	Valore
	`($.eventName=DeleteSecurity Group)}`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**
Valore predefinito	**`0`**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *`your-metric-name`* è...	Greater/Equal
rispetto a...	**`1`**

[CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.11, benchmark AWS CIS Foundations v1.4. 0/4.11, NIST.800-171.r2 3.14.6, 3.14.7, Profilo CRI v2. NIST.800-171.r2 2/DE. CM-01.03, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/PR. IR-01.02

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti. NACL vengono utilizzate come filtro dei pacchetti stateless per controllare il traffico in entrata e in uscita per sottoreti in un VPC.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche ai NACL. Il monitoraggio di queste modifiche aiuta a garantire che AWS risorse e servizi non vengano esposti involontariamente.

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire i passaggi di controllo esatti prescritti per il controllo 4.11 nel CIS Foundations Benchmark v1.4.0. AWS Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

> **Note**
>
> Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
> Il controllo dà luogo a `FAILED` risultati nei seguenti casi:
>
> - Non è configurato alcun percorso.
> - I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.
>
> Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:
>
> - Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
> - Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.
>
>   Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM

genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkAclEntry) || ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventN`

Campo	Valore
	`ame=ReplaceNetworkAclAssoci ation)}`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**
Valore predefinito	**`0`**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *`your-metric-name`* è...	Greater/Equal
rispetto a...	**`1`**

[CloudWatch.12] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gateway di rete

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.12, benchmark AWS CIS Foundations v1.4. 0/4.12, NIST.800-171.r2 3.3.1, 3.13.1, Profilo CRI v2 NIST.800-171.r2 . 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/RS. AN-07.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti. I gateway di rete sono necessari per inviare e ricevere traffico a una destinazione all'esterno di un VPC.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche ai gateway di rete. Il monitoraggio di tali modifiche garantisce che tutto il traffico in entrata e in uscita attraversa il bordo del VPC tramite un percorso controllato.

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 4.12 nel CIS Foundations Benchmark v1.2. AWS Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

> **Note**
>
> Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
> Il controllo dà luogo a `FAILED` risultati nei seguenti casi:
>
> - Non è configurato alcun percorso.
> - I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.
>
> Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:
>
> - Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
> - Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.
>
>   Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations

gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternet`

Campo	Valore
	`Gateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**
Valore predefinito	**`0`**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *`your-metric-name`* è...	Greater/Equal
rispetto a...	**`1`**

[CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.13, benchmark AWS CIS Foundations v1.4. 0/4.13, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, 3.14.6, 3.14.7, Profilo CRI v2. NIST.800-171.r2 NIST.800-171.r2 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-01.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se monitorate le chiamate API in tempo reale indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti. Le tabelle di routing instradano il traffico di rete tra le sottoreti e i gateway di rete.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche alle tabelle delle rotte. Il monitoraggio di queste modifiche garantisce che tutto il traffico VPC passi attraverso un percorso previsto.

Note

Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
Il controllo dà luogo a `FAILED` risultati nei seguenti casi:

- Non è configurato alcun percorso.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.

  Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM

genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Note

Il modello di filtro consigliato in queste fasi di riparazione è diverso dal modello di filtro nella guida CIS. I nostri filtri consigliati hanno come target solo gli eventi provenienti dalle chiamate API Amazon Elastic Compute Cloud (EC2).

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

   Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.
3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**
Valore predefinito	**`0`**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *`your-metric-name`* è...	Greater/Equal
rispetto a...	**`1`**

[CloudWatch.14] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche al VPC

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/3.14, benchmark AWS CIS Foundations v1.4. 0/4.14, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, 3.14.6, 3.14.7, NIST.800-171.r2 Profilo

CRI v2. NIST.800-171.r2 2/DE. CM-09.03, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti. Un account può contenere più VPC ed è possibile creare una connessione peer tra due VPC, consentendo l'instradamento del traffico di rete tra i VPC.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche ai VPC. Il monitoraggio di queste modifiche garantisce che i controlli di autenticazione e autorizzazione rimangano invariati.

Per eseguire questo controllo, Security Hub CSPM utilizza una logica personalizzata per eseguire i passaggi di controllo esatti prescritti per il controllo 4.14 nel CIS Foundations Benchmark v1.4.0. AWS Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

> **Note**
>
> Quando Security Hub CSPM esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. Multi-Region i sentieri potrebbero anche avere sede in una regione diversa.
> Il controllo dà luogo a `FAILED` risultati nei seguenti casi:
>
> - Non è configurato alcun percorso.
> - I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari `NO_DATA` a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.

  Come best practice, utilizzate gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Per impostazione predefinita, gli itinerari organizzativi sono percorsi multiregionali e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a `NO_DATA` per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando. `ListSubscriptionsByTopic` Altrimenti Security Hub CSPM genera `WARNING` risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service. Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta Creazione di un percorso nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta Creare un filtro metrico per un gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) || ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink) || ($.eventName=EnableVpcClassicLink)}`
Namespace metrico	**`LogMetrics`**
Valore del parametro	**`1`**
Valore predefinito	**`0`**

4. Crea un allarme basato sul filtro. Per istruzioni, consulta Creare un CloudWatch allarme basato su un filtro metrico del gruppo di log nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che *your-metric-name* è...	Greater/Equal
rispetto a...	**1**

[CloudWatch.15] gli CloudWatch allarmi dovrebbero avere azioni specificate configurate

Requisiti correlati: 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, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::CloudWatch::Alarm`

AWS Config regola: **`cloudwatch-alarm-action-check`**

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`alarmActionRequired`	Il controllo rileva `PASSED` se il parametro è impostato su `true` e l'allarme ha un'azione quando lo stato dell'allarme cambia a. `ALARM`	Booleano	Non personalizzabile	`true`

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`insufficientDataActionRequired`	Il controllo rileva `PASSED` se il parametro è impostato su `true` e l'allarme agisce quando lo stato dell'allarme cambia a`INSUFFICIENT_DATA` .	Booleano	`true` o `false`	`false`
`okActionRequired`	Il controllo rileva `PASSED` se il parametro è impostato su `true` e l'allarme agisce quando lo stato di allarme cambia a`OK`.	Booleano	`true` o `false`	`false`

Questo controllo verifica se un CloudWatch allarme Amazon ha almeno un'azione configurata per lo `ALARM` stato. Il controllo fallisce se l'allarme non ha un'azione configurata per lo `ALARM` stato. Facoltativamente, è possibile includere valori di parametri personalizzati per richiedere anche azioni di allarme per gli `OK` stati `INSUFFICIENT_DATA` or.

> **Note**
>
> Security Hub CSPM valuta questo controllo sulla CloudWatch base di allarmi metrici. Gli allarmi metrici possono far parte di allarmi compositi con le azioni specificate configurate. Il controllo genera `FAILED` risultati nei seguenti casi:
>
> - Le azioni specificate non sono configurate per un allarme metrico.
> - L'allarme metrico fa parte di un allarme composito in cui sono configurate le azioni specificate.

Questo controllo si concentra sul fatto che un CloudWatch allarme abbia un'azione di allarme configurata, mentre CloudWatch.17si concentra sullo stato di attivazione di un'azione di CloudWatch allarme.

Consigliamo azioni di CloudWatch allarme per avvisare automaticamente l'utente quando una metrica monitorata supera la soglia definita. Il monitoraggio degli allarmi consente di identificare attività insolite e di rispondere rapidamente ai problemi operativi e di sicurezza quando un allarme entra in uno stato specifico. Il tipo più comune di azione di allarme consiste nell'avvisare uno o più utenti inviando un messaggio a un argomento di Amazon Simple Notification Service (Amazon SNS).

Correzione

Per informazioni sulle azioni supportate dagli CloudWatch allarmi, consulta Azioni di allarme nella Amazon CloudWatch User Guide.

[CloudWatch.16] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato

Categoria: Identificazione > Registrazione

Requisiti correlati: 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 Profile v2. 2/ID. AM-08.03, Profilo CRI v2. 2/ID. AM-08.05, Profilo CRI v2. 2/PR. PS-04.01, Profilo CRI v2. 2/PR. PS-04.03

Gravità: media

Tipo di risorsa: `AWS::Logs::LogGroup`

AWS Config regola: **`cw-loggroup-retention-period-check`**

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`minRetentionTime`	Periodo minimo di conservazione in giorni per i gruppi di log CloudWatch	Enum	`365`, `400`, `545`, `731`,	`365`	

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
			1827, 3653		

Questo controllo verifica se un gruppo di CloudWatch log Amazon ha un periodo di conservazione di almeno il numero di giorni specificato. Il controllo fallisce se il periodo di conservazione è inferiore al numero specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione, Security Hub CSPM utilizza un valore predefinito di 365 giorni.

CloudWatch I log centralizzano i log di tutti i sistemi e le applicazioni Servizi AWS in un unico servizio altamente scalabile. Puoi usare CloudWatch Logs per monitorare, archiviare e accedere ai tuoi file di log da istanze Amazon Elastic Compute Cloud (EC2) AWS CloudTrail, Amazon Route 53 e altre fonti. Conservare i log per almeno 1 anno può aiutarti a rispettare gli standard di conservazione dei log.

Correzione

Per configurare le impostazioni di conservazione dei log, consulta Change log data retention in CloudWatch Logs nella Amazon CloudWatch User Guide.

[CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate

Categoria: Rilevamento > Servizi di rilevamento

Requisiti correlati: 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 Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01

Gravità: alta

Tipo di risorsa: `AWS::CloudWatch::Alarm`

AWS Config regola: **`cloudwatch-alarm-action-enabled-check`**

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le azioni di CloudWatch allarme sono attivate (`ActionEnabled`deve essere impostato su true). Il controllo fallisce se l'azione di allarme per un CloudWatch allarme è disattivata.

> **Note**
>
> Security Hub CSPM valuta questo controllo sulla CloudWatch base di allarmi metrici. Gli allarmi metrici possono far parte di allarmi compositi che hanno le azioni di allarme attivate. Il controllo genera `FAILED` risultati nei seguenti casi:
>
> - Le azioni specificate non sono configurate per un allarme metrico.
> - L'allarme metrico fa parte di un allarme composito con azioni di allarme attivate.

Questo controllo si concentra sullo stato di attivazione di un'azione di CloudWatch allarme, mentre CloudWatch.15si concentra sulla configurazione di `ALARM` un'azione in un CloudWatch allarme.

Le azioni di allarme avvisano automaticamente l'utente quando una metrica monitorata supera la soglia definita. Se l'azione di allarme è disattivata, non viene eseguita alcuna azione quando l'allarme cambia stato e non sarai avvisato delle modifiche nelle metriche monitorate. Ti consigliamo di attivare le azioni di CloudWatch allarme per aiutarti a rispondere rapidamente ai problemi operativi e di sicurezza.

Correzione

Per attivare un'azione CloudWatch di allarme (console)

1. Aprire la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, in Allarmi, scegli Tutti gli allarmi.
3. Seleziona l'allarme per il quale desideri attivare le azioni.
4. Per Azioni, scegli Azioni di allarme: nuove, quindi scegli Abilita.

Per ulteriori informazioni sull'attivazione delle azioni di CloudWatch allarme, consulta le azioni di allarme nella Amazon CloudWatch User Guide.

Controlli CSPM Security Hub per CodeArtifact

Questi controlli CSPM di Security Hub valutano il AWS CodeArtifact servizio e le risorse.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[CodeArtifact.1] i CodeArtifact repository devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::CodeArtifact::Repository`

AWS Configregola: `tagged-codeartifact-repository` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un AWS CodeArtifact repository ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il repository non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il repository non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse.

L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un CodeArtifact repository, consulta Etichettare un repository CodeArtifact nella Guida per l'utente. AWS CodeArtifact

Controlli CSPM Security Hub per CodeBuild

Questi controlli CSPM di Security Hub valutano il AWS CodeBuild servizio e le risorse.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili

Requisiti correlati: NIST.800-53.r5 SA-3, PCI DSS v3.2. 1/82.2.1, PCI DSS versione 4.0. 1/8.3.2, Profilo CRI v2. 2/PR. AA-04.01, Profilo CRI v2. 2/PR. DS-02.01

Categoria: Protezione > Sviluppo protetto

Severità: critica

Tipo di risorsa: `AWS::CodeBuild::Project`

Regola AWS Config : `codebuild-project-source-repo-url-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'URL del repository di origine Bitbucket di un AWS CodeBuild progetto contiene token di accesso personali o un nome utente e una password. Il controllo fallisce se l'URL del repository di origine Bitbucket contiene token di accesso personali o un nome utente e una password.

> **Note**
>
> Questo controllo valuta sia la fonte primaria che le fonti secondarie di un progetto di compilazione. CodeBuild Per ulteriori informazioni sulle fonti del progetto, consulta l'esempio di fonti di input e artefatti di output multipli nella Guida per l'AWS CodeBuild utente.

Sign-in le credenziali non devono essere archiviate o trasmesse in testo non crittografato o apparire nell'URL del repository di origine. Invece dei token di accesso personali o delle credenziali di accesso, dovresti accedere al tuo provider di origine e modificare l'URL del repository di origine in CodeBuild modo che contenga solo il percorso della posizione del repository Bitbucket. L'utilizzo di token di accesso personali o credenziali di accesso potrebbe comportare l'esposizione involontaria dei dati o l'accesso non autorizzato.

Correzione

Puoi aggiornare il tuo CodeBuild progetto per utilizzare OAuth.

Per rimuovere l'autenticazione di base/(GitHub) Personal Access Token dal sorgente del progetto CodeBuild

1. Apri la CodeBuild console all'indirizzo https://console.aws.amazon.com/codebuild/.
2. Scegliere il progetto di compilazione contenente i token di accesso personali o un nome utente e una password.
3. Da Edit (Modifica), scegliere Source (Sorgente).
4. Scegli Disconnetti da GitHub /Bitbucket.
5. Scegli Connetti tramite OAuth, quindi scegli Connetti GitHub a/Bitbucket.
6. Quando richiesto, scegliere authorize as appropriate (autorizza come appropriato).
7. Riconfigurare l'URL repository) e le impostazioni di configurazione aggiuntive, se necessario.

8. Scegliere Update source (Aggiorna origine).

Per ulteriori informazioni, consulta gli esempi basati su casi CodeBuild d'uso nella Guida per l'utente.AWS CodeBuild

[CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato

Requisiti correlati: NIST.800-53.r5 IA-5 (7) NIST.800-53.r5 SA-3, PCI DSS v3.2. 1/82.1, PCI DSS versione 4.0. 1/8.3.2, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-06.04

Categoria: Protezione > Sviluppo protetto

Severità: critica

Tipo di risorsa: `AWS::CodeBuild::Project`

Regola AWS Config : `codebuild-project-envvar-awscred-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il progetto contiene le variabili di ambiente `AWS_ACCESS_KEY_ID` e `AWS_SECRET_ACCESS_KEY`.

Le credenziali di autenticazione `AWS_ACCESS_KEY_ID` e `AWS_SECRET_ACCESS_KEY` non devono mai essere memorizzate in testo non crittografato, in quanto ciò potrebbe comportare l'esposizione non intenzionale dei dati e l'accesso non autorizzato.

Correzione

Per rimuovere le variabili di ambiente da un CodeBuild progetto, consulta Modificare le impostazioni di un progetto di build AWS CodeBuild nella Guida per l'AWS CodeBuild utente. Assicurati che non sia selezionato nulla per le variabili di ambiente.

Puoi memorizzare le variabili di ambiente con valori sensibili nel AWS Systems Manager Parameter Store o AWS Secrets Manager recuperarle dalle specifiche di build. Per istruzioni, consulta la casella denominata Importante nella sezione Ambiente della Guida per l'AWS CodeBuild utente.

[CodeBuild.3] I log CodeBuild S3 devono essere crittografati

Requisiti correlati: 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, NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/10.3.2, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: bassa

Tipo di risorsa: `AWS::CodeBuild::Project`

Regola AWS Config : `codebuild-project-s3-logs-encrypted`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i log di Amazon S3 per un AWS CodeBuild progetto sono crittografati. Il controllo fallisce se la crittografia è disattivata per i log S3 di un progetto. CodeBuild

La crittografia dei dati inattivi è una best practice consigliata per aggiungere un livello di gestione degli accessi ai dati. La crittografia dei registri inattivi riduce il rischio che un utente non autenticato da acceda AWS ai dati archiviati su disco. Aggiunge un altro set di controlli di accesso per limitare la capacità degli utenti non autorizzati di accedere ai dati.

Correzione

Per modificare le impostazioni di crittografia per i log CodeBuild del progetto S3, consulta Modificare le impostazioni di un progetto di build AWS CodeBuild nella Guida per l'AWS CodeBuild utente.

[CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]

Requisiti correlati: 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), (8), NIST.800-53.r5 SI-3 (20) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), CRI Profile v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. IR-04.01, Profilo CRI v2. 2/PR. PS-04.02

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::CodeBuild::Project`

Regola AWS Config : `codebuild-project-logging-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un ambiente di CodeBuild progetto ha almeno un'opzione di registro, su S3 o sui CloudWatch log abilitati. Questo controllo fallisce se un ambiente di CodeBuild progetto non ha almeno un'opzione di registro abilitata.

Dal punto di vista della sicurezza, la registrazione è una funzionalità importante per consentire future attività di analisi forense in caso di incidenti di sicurezza. La correlazione delle anomalie nei CodeBuild progetti con il rilevamento delle minacce può aumentare la fiducia nell'accuratezza di tali rilevamenti di minacce.

Correzione

Per ulteriori informazioni su come configurare le impostazioni CodeBuild del registro di progetto, consulta Creare un progetto di compilazione (console) nella Guida per l'utente. CodeBuild

[CodeBuild.7] le esportazioni dei gruppi di CodeBuild report devono essere crittografate quando sono inattive

Requisiti correlati: CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::CodeBuild::ReportGroup`

Regola AWS Config : `codebuild-report-group-encrypted-at-rest`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i risultati dei test di un gruppo di AWS CodeBuild report esportati in un bucket Amazon Simple Storage Service (Amazon S3) sono crittografati quando sono inattivi. Il controllo fallisce se l'esportazione del gruppo di report non è crittografata quando è inattivo.

I dati inattivi si riferiscono ai dati archiviati in uno spazio di archiviazione persistente e non volatile per qualsiasi durata. La crittografia dei dati inutilizzati consente di proteggerne la riservatezza, riducendo il rischio che un utente non autorizzato possa accedervi.

Correzione

Per crittografare l'esportazione del gruppo di report in S3, consulta Aggiornare un gruppo di report nella Guida per l'utente.AWS CodeBuild

Controlli CSPM di Security Hub per Amazon Profiler CodeGuru

Questi controlli CSPM di Security Hub valutano il servizio e le risorse Amazon CodeGuru Profiler.

Questi controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::CodeGuruProfiler::ProfilingGroup`

Regola AWS Config : `codeguruprofiler-profiling-group-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un gruppo di CodeGuru profilazione Amazon Profiler dispone di tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se il gruppo di profilazione non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredKeyTags` Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di profilazione non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un gruppo di CodeGuru profilazione Profiler, consulta Tagging profiling groups nella Amazon CodeGuru Profiler User Guide.

Controlli CSPM di Security Hub per Amazon Reviewer CodeGuru

Questi controlli CSPM di Security Hub valutano il servizio e le CodeGuru risorse Amazon Reviewer.

Questi controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::CodeGuruReviewer::RepositoryAssociation`

Regola AWS Config : `codegurureviewer-repository-association-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un'associazione di repository Amazon CodeGuru Reviewer ha tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se l'associazione di repository non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredKeyTags` Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'associazione del repository non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse.

L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un'associazione di repository CodeGuru Reviewer, consulta Tagging a repository association nella Amazon CodeGuru Reviewer User Guide.

Controlli CSPM del Security Hub per Amazon Cognito

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse di Amazon Cognito. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::Cognito::UserPool`

Regola AWS Config : cognito-user-pool-advanced-security-enabled

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`SecurityMode`	La modalità di applicazione della protezione dalle minacce verificata dal controllo.	Stringa	`AUDIT`, `ENFORCED`	`ENFORCED`

Questo controllo verifica se un pool di utenti di Amazon Cognito ha la protezione dalle minacce attivata con la modalità di imposizione impostata sulla piena funzionalità per l'autenticazione standard. Il controllo fallisce se nel pool di utenti la protezione dalle minacce è disattivata o se la modalità di imposizione non è impostata sulla funzionalità completa per l'autenticazione standard. A meno che non si forniscano valori di parametro personalizzati, Security Hub CSPM utilizza il valore predefinito di `ENFORCED` for enforcement mode impostato su full function per l'autenticazione standard.

Dopo aver creato un pool di utenti Amazon Cognito, puoi attivare la protezione dalle minacce e personalizzare le azioni intraprese in risposta a diversi rischi. In alternativa, puoi utilizzare la modalità di controllo per raccogliere metriche sui rischi rilevati senza applicare alcuna mitigazione della sicurezza. In modalità di controllo, la protezione dalle minacce pubblica i parametri su Amazon. CloudWatch Puoi visualizzare le metriche dopo che Amazon Cognito ha generato il suo primo evento.

Correzione

Per informazioni sull'attivazione della protezione dalle minacce per un pool di utenti di Amazon Cognito, consulta Sicurezza avanzata con protezione dalle minacce nella Amazon Cognito Developer Guide.

[Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate

Requisiti correlati: CRI Profile v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-04.01

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: `AWS::Cognito::IdentityPool`

Regola AWS Config : cognito-identity-pool-unauth-access-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un pool di identità di Amazon Cognito è configurato per consentire identità non autenticate. Il controllo fallisce se l'accesso guest è attivato (il `AllowUnauthenticatedIdentities` parametro è impostato su`true`) per il pool di identità.

Se un pool di identità di Amazon Cognito consente identità non autenticate, il pool di identità fornisce AWS credenziali temporanee agli utenti che non si sono autenticati tramite un provider di identità (ospiti). Ciò crea rischi per la sicurezza perché consente l'accesso anonimo alle risorse. AWS Se disattivi l'accesso come ospite, puoi contribuire a garantire che solo gli utenti correttamente autenticati possano accedere alle tue AWS risorse, riducendo il rischio di accessi non autorizzati e potenziali violazioni della sicurezza. Come best practice, un pool di identità dovrebbe richiedere l'autenticazione tramite provider di identità supportati. Se è necessario un accesso non autenticato, è importante limitare attentamente le autorizzazioni per le identità non autenticate e rivederne e monitorarne regolarmente l'utilizzo.

Correzione

Per informazioni sulla disattivazione dell'accesso guest per un pool di identità di Amazon Cognito, consulta Attivare o disattivare l'accesso guest nella Amazon Cognito Developer Guide.

[Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate

Requisiti correlati: CRI Profile v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::Cognito::UserPool`

Regola AWS Config : cognito-user-pool-password-policy-check

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`minLength`	Il numero minimo di caratteri che una password deve contenere.	Numero intero	Da 8 a 99	8
`requireLowercase`	Richiede almeno un carattere minuscolo in una password.	Booleano	`True`, `False`	`True`
`requireUppercase`	Richiede almeno un carattere maiuscolo in una password.	Booleano	`True`, `False`	`True`
`requireNumbers`	Richiede almeno un numero in una password.	Booleano	`True`, `False`	`True`
`requireSymbols`	Richiede almeno un simbolo in una password.	Booleano	`True`, `False`	`True`
`temporaryPasswordValidity`	Il numero massimo di giorni in cui una password può esistere prima della scadenza.	Numero intero	Da 1 a 365	7

Questo controllo verifica se la politica delle password per un pool di utenti di Amazon Cognito richiede l'uso di password complesse, in base alle impostazioni consigliate per le politiche di password. Il controllo ha esito negativo se la politica delle password per il pool di utenti non richiede password complesse. Facoltativamente, è possibile specificare valori personalizzati per le impostazioni dei criteri controllate dal controllo.

Le password complesse sono una best practice di sicurezza per i pool di utenti di Amazon Cognito. Le password deboli possono esporre le credenziali degli utenti a sistemi che indovinano le password e cercano di accedere ai dati. Questo vale in particolare per le applicazioni aperte a Internet. Le politiche relative alle password sono un elemento centrale della sicurezza degli elenchi degli utenti. Utilizzando una politica in materia di password, è possibile configurare un pool di utenti in modo che

richieda la complessità delle password e altre impostazioni conformi agli standard e ai requisiti di sicurezza.

Correzione

Per informazioni sulla creazione o l'aggiornamento della politica di password per un pool di utenti di Amazon Cognito, consulta Aggiungere i requisiti di password del pool di utenti nella Amazon Cognito Developer Guide.

[Cognito.4] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::Cognito::UserPool`

Regola AWS Config : cognito-userpool-cust-auth-threat-full-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un pool di utenti di Amazon Cognito ha la protezione dalle minacce attivata con la modalità di imposizione impostata sulla funzionalità completa per l'autenticazione personalizzata. Il controllo fallisce se il pool di utenti ha la protezione dalle minacce disabilitata o se la modalità di imposizione non è impostata sulla funzionalità completa per l'autenticazione personalizzata.

La protezione dalle minacce, precedentemente denominata funzionalità di sicurezza avanzate, è un insieme di strumenti di monitoraggio delle attività indesiderate nel pool di utenti e strumenti di configurazione per arrestare automaticamente le attività potenzialmente dannose. Dopo aver creato un pool di utenti Amazon Cognito, puoi attivare la protezione dalle minacce con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata e personalizzare le azioni intraprese in risposta a diversi rischi. Full-function la modalità include una serie di reazioni automatiche per rilevare attività indesiderate e password compromesse.

Correzione

Per informazioni sull'attivazione della protezione dalle minacce per un pool di utenti di Amazon Cognito, consulta Sicurezza avanzata con protezione dalle minacce nella Amazon Cognito Developer Guide.

[Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito

Categoria: Protezione > Gestione sicura degli accessi > autenticazione Multi-factor

Gravità: media

Tipo di risorsa: `AWS::Cognito::UserPool`

Regola AWS Config : cognito-user-pool-mfa-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un pool di utenti di Amazon Cognito configurato con una politica di accesso con sola password ha l'autenticazione a più fattori (MFA) abilitata. Il controllo ha esito negativo se il pool di utenti configurato con un criterio di accesso basato sulla sola password non ha l'MFA abilitata.

Multi-factor l'autenticazione (MFA) aggiunge un fattore di autenticazione qualcosa che hai al fattore qualcosa che conosci (in genere nome utente e password). Per gli utenti federati, Amazon Cognito delega l'autenticazione al provider di identità (IdP) e non offre fattori di autenticazione aggiuntivi. Tuttavia, se si dispone di utenti locali con autenticazione tramite password, la configurazione dell'MFA per il pool di utenti ne aumenta la sicurezza.

> **Note**
>
> Questo controllo non è applicabile agli utenti federati e agli utenti che accedono con fattori privi di password.

Correzione

Per informazioni su come configurare l'MFA per un pool di utenti di Amazon Cognito, consulta Adding MFA a un pool di utenti nella Amazon Cognito Developer Guide.

[Cognito.6] I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata

Categoria: Proteggi > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: media

Tipo di risorsa: `AWS::Cognito::UserPool`

Regola AWS Config : cognito-user-pool-deletion-protection-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un pool di utenti di Amazon Cognito ha la protezione da eliminazione abilitata. Il controllo fallisce se la protezione da eliminazione è disabilitata per il pool di utenti.

La protezione dall'eliminazione aiuta a garantire che il pool di utenti non venga eliminato accidentalmente. Quando si configura un pool di utenti con protezione dall'eliminazione, il pool non può essere eliminato da nessun utente. La protezione da eliminazione impedisce di richiedere l'eliminazione di un pool di utenti a meno che non si modifichi prima il pool e si disattivi la protezione dall'eliminazione.

Correzione

Per configurare la protezione dall'eliminazione per un pool di utenti di Amazon Cognito, consulta Protezione dall'eliminazione del pool di utenti nella Amazon Cognito Developer Guide.

Controlli CSPM Security Hub per AWS Config

Questi controlli CSPM di Security Hub valutano il AWS Config servizio e le risorse.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse

> **Note**
>
> Quando Security Hub CSPM e Security Hub sono abilitati, la Config.1 regola avrà sempre lo stato PASSATA. Questo perché Security Hub CSPM ha accesso diretto agli elementi di configurazione tramite un registratore di configurazione collegato al servizio. Il parametro per questo controllo non è applicabile in quanto il registratore di configurazione interno collegato al servizio viene creato automaticamente con il ruolo collegato al servizio. AWS Config Per ulteriori informazioni, consulta Utilizzo del registratore di configurazione collegato al servizio. I controlli multicloud (come i controlli di Azure) e la registrazione delle risorse associata non vengono presi in considerazione nelle valutazioni. Config.1 Gli standard multicloud utilizzano sempre un registratore di configurazione interno collegato ai servizi che il connettore

multicloud CSPM configura automaticamente, indipendentemente dallo stato di abilitazione del Security Hub. Poiché la registrazione multicloud è completamente gestita dal connettore, non influisce sullo stato di conformità. Config.1 Config.1 valuta solo la configurazione della registrazione AWS delle risorse.

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/3.3, benchmark AWS CIS Foundations v1.2. 0/2.5, benchmark AWS CIS Foundations v1.4. 0/3.5, benchmark AWS CIS Foundations v3.0. 0/3.3, NIST.800-53.r5 CM-6 (1) NIST.800-53.r5 CM-3, NIST.800-53.r5 CM-8 (2) NIST.800-53.r5 CM-8, PCI DSS versione 3.2. 1/105.2, PCI DSS versione 3.2. 1/11.5, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Identificazione > Inventario

Severità: critica

Tipo di risorsa: `AWS::::Account`

AWS Config regola: Nessuna (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`includeConfigServiceLinkedRoleCheck`	Il controllo non valuta se AWS Config utilizza il ruolo collegato al servizio se il parametro è impostato su. `false`	Booleano	`true` o `false`	`true`

Questo controllo verifica se AWS Config è abilitato nell'account corrente Regione AWS, registra tutte le risorse che corrispondono ai controlli abilitati nella regione corrente e utilizza il ruolo collegato al servizio AWS Config. Il nome del ruolo collegato al servizio è. AWSServiceRoleForConfig Se non si utilizza il ruolo collegato al servizio e non si imposta il `includeConfigServiceLinkedRoleCheck`

parametro su`false`, il controllo ha esito negativo perché altri ruoli potrebbero non disporre delle autorizzazioni necessarie per AWS Config registrare accuratamente le risorse.

Il AWS Config servizio esegue la gestione della configurazione delle AWS risorse supportate nell'account e fornisce i file di registro. Le informazioni registrate includono l'elemento di configurazione (AWS risorsa), le relazioni tra gli elementi di configurazione e qualsiasi modifica alla configurazione all'interno delle risorse. Le risorse globali sono risorse disponibili in qualsiasi regione.

Il controllo viene valutato come segue:

- Se la regione corrente è impostata come regione di aggregazione, il controllo produce `PASSED` risultati solo se vengono registrate risorse globali AWS Identity and Access Management (IAM) (se sono stati abilitati i controlli che li richiedono).
- Se la regione corrente è impostata come regione collegata, il controllo non valuta se le risorse globali IAM sono registrate.
- Se la regione corrente non è nel tuo aggregatore o se l'aggregazione tra regioni non è impostata nel tuo account, il controllo produce `PASSED` risultati solo se le risorse globali IAM sono registrate (se hai abilitato i controlli che li richiedono).

I risultati del controllo non sono influenzati dalla scelta della registrazione giornaliera o continua delle modifiche allo stato delle risorse in. AWS Config Tuttavia, i risultati di questo controllo possono cambiare quando vengono rilasciati nuovi controlli se è stata configurata l'attivazione automatica di nuovi controlli o se si dispone di una politica di configurazione centrale che abilita automaticamente nuovi controlli. In questi casi, se non si registrano tutte le risorse, è necessario configurare la registrazione per le risorse associate ai nuovi controlli per ricevere un `PASSED` risultato.

I controlli di sicurezza CSPM di Security Hub funzionano come previsto solo se si abilita AWS Config in tutte le regioni e si configura la registrazione delle risorse per i controlli che la richiedono.

> **Note**
>
> Config.1 richiede che AWS Config sia abilitato in tutte le regioni in cui si utilizza Security Hub CSPM.
> Poiché Security Hub CSPM è un servizio regionale, il controllo eseguito per questo controllo valuta solo la regione corrente per l'account.
> Per consentire i controlli di sicurezza sulle risorse globali IAM in una regione, è necessario registrare le risorse globali IAM in quella regione. Le regioni in cui non sono registrate risorse globali IAM riceveranno un `PASSED` risultato predefinito per i controlli che controllano le

risorse globali IAM. Poiché le risorse globali IAM sono identiche in tutte le aree Regioni AWS, ti consigliamo di registrare le risorse globali IAM solo nella regione principale (se l'aggregazione interregionale è abilitata nel tuo account). Le risorse IAM verranno registrate solo nella regione in cui è attivata la registrazione delle risorse globali.
I tipi di risorse IAM registrati a livello globale che AWS Config supportano sono utenti, gruppi, ruoli e politiche gestite dai clienti IAM. Puoi prendere in considerazione la possibilità di disabilitare i controlli CSPM di Security Hub che controllano questi tipi di risorse nelle regioni in cui la registrazione globale delle risorse è disattivata. Per ulteriori informazioni, consulta Controlli consigliati da disabilitare in Security Hub CSPM.

Correzione

Nella regione principale e nelle regioni che non fanno parte di un aggregatore, registra tutte le risorse necessarie per i controlli abilitati nella regione corrente, incluse le risorse globali IAM se hai abilitato controlli che richiedono risorse globali IAM.

Nelle regioni collegate, è possibile utilizzare qualsiasi modalità di AWS Config registrazione, purché si registrino tutte le risorse che corrispondono ai controlli abilitati nella regione corrente. Nelle regioni collegate, se hai abilitato i controlli che richiedono la registrazione di risorse globali IAM, non riceverai alcun `FAILED` risultato (la registrazione di altre risorse è sufficiente).

Il `StatusReasons` campo nell'`Compliance`oggetto della ricerca può aiutarti a determinare il motivo per cui hai fallito la ricerca per questo controllo. Per ulteriori informazioni, consulta Dettagli sulla conformità per i risultati del controllo.

Per un elenco delle risorse da registrare per ogni controllo, vedereRichiesto AWS Config risorse per i risultati del controllo. Per informazioni generali sull'attivazione AWS Config e la configurazione della registrazione delle risorse, vedereAttivazione e configurazione AWS Config per Security Hub CSPM.

Controlli CSPM del Security Hub per Amazon Connect

Questi controlli CSPM di Security Hub valutano il servizio e le risorse Amazon Connect.

Questi controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::CustomerProfiles::ObjectType`

Regola AWS Config : `customerprofiles-object-type-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un tipo di oggetto Amazon Connect Customer Profiles ha tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se il tipo di oggetto non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il tipo di oggetto non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per

ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un tipo di oggetto Customer Profiles, consulta Aggiungere tag alle risorse in Amazon Connect Customer nella Connect Customer Administrator Guide.

[Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata

Requisiti correlati: CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::Connect::Instance`

AWS Config regola: connect-instance-logging-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istanza Connect Customer è configurata per generare e archiviare i log di flusso in un gruppo di CloudWatch log Amazon. Il controllo fallisce se l'istanza Connect Customer non è configurata per generare e archiviare i log di flusso in un gruppo di CloudWatch log.

I log di flusso dei clienti di Amazon Connect forniscono dettagli in tempo reale sugli eventi nei flussi di clienti Amazon Connect. Un flusso definisce l'esperienza del cliente con un contact center Amazon Connect dall'inizio alla fine. Per impostazione predefinita, quando crei una nuova istanza

Amazon Connect Customer, viene creato automaticamente un gruppo di CloudWatch log Amazon per archiviare i log di flusso per l'istanza. I log di flusso possono aiutarti ad analizzare i flussi, trovare errori e monitorare le metriche operative. Puoi anche impostare avvisi per eventi specifici che possono verificarsi in un flusso.

Correzione

Per informazioni sull'abilitazione dei log di flusso per un'istanza Amazon Connect Customer Customer, consulta Abilitare i log di flusso dei clienti Amazon Connect in un gruppo di CloudWatch log Amazon Connect nella Connect Customer Administrator Guide.

Controlli CSPM del Security Hub per Amazon Data Firehose

Questi controlli CSPM di Security Hub valutano il servizio e le risorse Amazon Data Firehose.

Questi controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi

Requisiti correlati: 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, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::KinesisFirehose::DeliveryStream`

Regola AWS Config : `kinesis-firehose-delivery-stream-encrypted`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un flusso di distribuzione di Amazon Data Firehose è crittografato quando è inattivo con crittografia lato server. Questo controllo fallisce se un flusso di distribuzione Firehose non è crittografato a riposo con la crittografia lato server.

Server-side la crittografia è una funzionalità dei flussi di distribuzione di Amazon Data Firehose che crittografa automaticamente i dati prima che siano inattivi utilizzando una chiave creata in (). AWS

Key Management Service AWS KMS I dati vengono crittografati prima di essere scritti nel layer di storage stream Data Firehose e decrittografati dopo essere stati recuperati dallo storage. Ciò consente di rispettare i requisiti normativi e di migliorare la sicurezza dei dati.

Correzione

Per abilitare la crittografia lato server sui flussi di distribuzione Firehose, consulta la sezione Protezione dei dati in Amazon Data Firehose nella Amazon Data Firehose Developer Guide.

Controlli CSPM Security Hub per AWS Database Migration Service

Questi AWS Security Hub CSPM controlli valutano AWS Database Migration Service (AWS DMS) e AWS DMS le risorse. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[DMS.1] Le istanze di replica del Database Migration Service non devono essere pubbliche

Requisiti correlati: 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. 1/1.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 1/1.3.6, PCI DSS versione 4.0. 1/1.4.4, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: `AWS::DMS::ReplicationInstance`

Regola AWS Config : dms-replication-not-public

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se le istanze di AWS DMS replica sono pubbliche. A tale scopo, esamina il valore del campo. `PubliclyAccessible`

Un'istanza di replica privata ha un indirizzo IP privato a cui non è possibile accedere al di fuori della rete di replica. Un'istanza di replica deve avere un indirizzo IP privato quando i database di origine e di destinazione si trovano nella stessa rete. La rete deve inoltre essere connessa al VPC dell'istanza di replica utilizzando una VPN o un Direct Connect peering VPC. Per ulteriori informazioni sulle istanze di replica pubbliche e private, consulta Istanze di replica pubbliche e private nella Guida per l'utente.AWS Database Migration Service

È inoltre necessario assicurarsi che l'accesso alla configurazione dell' AWS DMS istanza sia limitato ai soli utenti autorizzati. A tale scopo, limita le autorizzazioni IAM degli utenti per modificare AWS DMS impostazioni e risorse.

Correzione

Non è possibile modificare l'impostazione di accesso pubblico per un'istanza di replica DMS dopo averla creata. Per modificare l'impostazione di accesso pubblico, elimina l'istanza corrente e quindi ricreala. Non selezionare l'opzione Accessibile pubblicamente.

[DMS.2] I certificati DMS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::DMS::Certificate`

AWS Config regola: `tagged-dms-certificate` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	I tag fanno distinzione tra maiuscole e minuscole			

Questo controllo verifica se un AWS DMS certificato ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il certificato non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il certificato non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un certificato DMS, consulta Tagging resources AWS Database Migration Service nella Guida per l'utente.AWS Database Migration Service

[DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::DMS::EventSubscription`

AWS Config regola: `tagged-dms-eventsubscription` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se una sottoscrizione a un AWS DMS evento ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la sottoscrizione all'evento non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la sottoscrizione all'evento non è contrassegnata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un abbonamento a un evento DMS, consulta Tagging resources AWS Database Migration Service nella Guida per l'utente.AWS Database Migration Service

[DMS.4] Le istanze di replica DMS devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::DMS::ReplicationInstance`

AWS Config regola: `tagged-dms-replicationinstance` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfan	`No default value`

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	I tag fanno distinzione tra maiuscole e minuscole		o i requisiti AWS .	

Questo controllo verifica se un'istanza di AWS DMS replica ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo ha esito negativo se l'istanza di replica non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'istanza di replica non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'istanza di replica DMS, consulta Tagging resources nella AWS Database Migration Service Guida per l'utente.AWS Database Migration Service

[DMS.5] I sottoreti di replica DMS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::DMS::ReplicationSubnetGroup`

AWS Config regola: `tagged-dms-replicationsubnetgroup` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un gruppo di AWS DMS sottoreti di replica dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo ha esito negativo se il gruppo di sottorete di replica non dispone di chiavi di tag o se non dispone di tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di sottorete di replica non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli

accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un sottogruppo di replica DMS, consulta Tagging resources nella Guida per l'utente. AWS Database Migration ServiceAWS Database Migration Service

[DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato

Requisiti correlati: 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. 1/6.3.3, Profilo CRI v2. 2/ID. RA-01.03, Profilo CRI v2. 2/PR. PS-02.01

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: `AWS::DMS::ReplicationInstance`

Regola AWS Config : dms-auto-minor-version-upgrade-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'aggiornamento automatico della versione secondaria è abilitato per un'istanza di AWS DMS replica. Il controllo fallisce se l'aggiornamento automatico della versione secondaria non è abilitato per un'istanza di replica DMS.

DMS fornisce l'aggiornamento automatico delle versioni secondarie a ciascun motore di replica supportato, in modo da mantenere aggiornata l'istanza di replica. Le versioni minori possono introdurre nuove funzionalità software, correzioni di bug, patch di sicurezza e miglioramenti delle prestazioni. Abilitando l'aggiornamento automatico delle versioni secondarie sulle istanze di replica DMS, gli aggiornamenti minori vengono applicati automaticamente durante la finestra di manutenzione o immediatamente se viene selezionata l'opzione Applica modifiche immediatamente.

Correzione

Per abilitare l'aggiornamento automatico delle versioni secondarie sulle istanze di replica DMS, vedere Modifica di un'istanza di replica nella Guida per l'utente.AWS Database Migration Service

[DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata

Requisiti correlati: 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. 1/10.4.2, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::DMS::ReplicationTask`

Regola AWS Config : dms-replication-task-targetdb-logging

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione è abilitata con il livello di gravità minimo di `LOGGER_SEVERITY_DEFAULT` per le attività di replica DMS e. `TARGET_APPLY` `TARGET_LOAD` Il controllo ha esito negativo se la registrazione non è abilitata per queste attività o se il livello di gravità minimo è inferiore a. `LOGGER_SEVERITY_DEFAULT`

DMS utilizza Amazon CloudWatch per registrare le informazioni durante il processo di migrazione. Utilizzando le impostazioni delle attività di registrazione, puoi specificare quali attività dei componenti vengono registrate e quante informazioni vengono registrate. È necessario specificare la registrazione per le seguenti attività:

- `TARGET_APPLY`: i dati e le istruzioni DDL (Data Definition Language) vengono applicati al database di destinazione.
- `TARGET_LOAD`: i dati vengono caricati nel database di destinazione.

La registrazione svolge un ruolo fondamentale nelle attività di replica DMS poiché consente il monitoraggio, la risoluzione dei problemi, il controllo, l'analisi delle prestazioni, il rilevamento e il ripristino degli errori, nonché l'analisi e il reporting cronologici. Contribuisce a garantire la corretta replica dei dati tra database, mantenendo al contempo l'integrità dei dati e la conformità ai requisiti normativi. Livelli di registrazione diversi da `DEFAULT` sono raramente necessari per questi componenti durante la risoluzione dei problemi. Si consiglia di mantenere il livello di registrazione come `DEFAULT` per questi componenti, a meno che non venga espressamente richiesto di modificarlo entro. Supporto Un livello di registrazione minimo `DEFAULT` garantisce che i messaggi informativi, gli avvisi e i messaggi di errore vengano scritti nei log. Questo controllo verifica se il livello di registrazione è almeno uno dei seguenti per le attività di replica precedenti:, o. `LOGGER_SEVERITY_DEFAULT` `LOGGER_SEVERITY_DEBUG` `LOGGER_SEVERITY_DETAILED_DEBUG`

Correzione

Per abilitare la registrazione per le attività di replica DMS del database di destinazione, vedere Visualizzazione e gestione dei AWS DMS registri delle attività nella Guida per l'utente.AWS Database Migration Service

[DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata

Requisiti correlati: 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. 1/10.4.2, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::DMS::ReplicationTask`

Regola AWS Config : dms-replication-task-sourcedb-logging

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione è abilitata con il livello di gravità minimo di LOGGER_SEVERITY_DEFAULT per le attività di replica DMS e. SOURCE_CAPTURE SOURCE_UNLOAD Il controllo ha esito negativo se la registrazione non è abilitata per queste attività o se il livello di gravità minimo è inferiore a. LOGGER_SEVERITY_DEFAULT

DMS utilizza Amazon CloudWatch per registrare le informazioni durante il processo di migrazione. Utilizzando le impostazioni delle attività di registrazione, puoi specificare quali attività dei componenti vengono registrate e quante informazioni vengono registrate. È necessario specificare la registrazione per le seguenti attività:

- SOURCE_CAPTURE— I dati di replica continua o acquisizione dei dati di modifica (CDC) vengono acquisiti dal database o dal servizio di origine e passati al componente del SORTER servizio.
- SOURCE_UNLOAD— I dati vengono scaricati dal database o dal servizio di origine durante il pieno caricamento.

La registrazione svolge un ruolo fondamentale nelle attività di replica DMS poiché consente il monitoraggio, la risoluzione dei problemi, il controllo, l'analisi delle prestazioni, il rilevamento e il ripristino degli errori, nonché l'analisi e il reporting cronologici. Contribuisce a garantire la corretta replica dei dati tra database, mantenendo al contempo l'integrità dei dati e la conformità ai requisiti normativi. Livelli di registrazione diversi da DEFAULT sono raramente necessari per questi componenti durante la risoluzione dei problemi. Si consiglia di mantenere il livello di registrazione come DEFAULT per questi componenti, a meno che non venga espressamente richiesto di modificarlo entro. Supporto Un livello di registrazione minimo DEFAULT garantisce che i messaggi informativi, gli avvisi e i messaggi di errore vengano scritti nei log. Questo controllo verifica se il livello di registrazione è almeno uno dei seguenti per le attività di replica precedenti:, o. LOGGER_SEVERITY_DEFAULT LOGGER_SEVERITY_DEBUG LOGGER_SEVERITY_DETAILED_DEBUG

Correzione

Per abilitare la registrazione per le attività di replica DMS del database di origine, vedere Visualizzazione e gestione dei AWS DMS registri delle attività nella Guida per l'utente.AWS Database Migration Service

[DMS.9] Gli endpoint DMS devono utilizzare SSL

Requisiti correlati: 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. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::DMS::Endpoint`

Regola AWS Config : dms-endpoint-ssl-configured

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS DMS endpoint utilizza una connessione SSL. Il controllo fallisce se l'endpoint non utilizza SSL.

SSL/TLS le connessioni forniscono un livello di sicurezza crittografando le connessioni tra le istanze di replica DMS e il database. L'utilizzo dei certificati fornisce un ulteriore livello di sicurezza convalidando che la connessione venga stabilita al database previsto. A tale scopo, verifica il certificato del server che viene installato automaticamente su tutte le istanze di database fornite. Abilitando la connessione SSL sugli endpoint DMS, proteggete la riservatezza dei dati durante la migrazione.

Correzione

Per aggiungere una connessione SSL a un endpoint DMS nuovo o esistente, consulta Using SSL with nella Guida per l'utente. AWS Database Migration ServiceAWS Database Migration Service

[DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata

Requisiti correlati: NIST.800-53.r5 AC-2,,, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-17 NIST.800-53.r5 IA-2, NIST.800-53.r5 IA-5 PCI DSS v4.0. 1/7.3.1, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: `AWS::DMS::Endpoint`

Regola AWS Config : dms-neptune-iam-authorization-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS DMS endpoint per un database Amazon Neptune è configurato con l'autorizzazione IAM. Il controllo fallisce se l'endpoint DMS non ha l'autorizzazione IAM abilitata.

AWS Identity and Access Management (IAM) fornisce un controllo granulare degli accessi su tutto il territorio. AWS Con IAM, puoi specificare chi può accedere a quali servizi e risorse e in quali condizioni. Con le policy IAM, gestisci le autorizzazioni per la tua forza lavoro e i tuoi sistemi per garantire le autorizzazioni con privilegi minimi. Abilitando l'autorizzazione IAM sugli AWS DMS endpoint per i database Neptune, puoi concedere privilegi di autorizzazione agli utenti IAM utilizzando un ruolo di servizio specificato dal parametro. `ServiceAccessRoleARN`

Correzione

Per abilitare l'autorizzazione IAM sugli endpoint DMS per i database Neptune, consulta Using Amazon Neptune come target nella Guida per l'utente. AWS Database Migration ServiceAWS Database Migration Service

[DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato

Requisiti correlati: 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. 1/7.3.1, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-04.01, Profilo CRI v2. 2/PR. DS-01.01

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: `AWS::DMS::Endpoint`

Regola AWS Config : dms-mongo-db-authentication-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS DMS endpoint per MongoDB è configurato con un meccanismo di autenticazione. Il controllo fallisce se non è impostato un tipo di autenticazione per l'endpoint.

AWS Database Migration Service supporta due metodi di autenticazione per MongoDB: per MongoDB versione 2.x e MONGODB-CRper MongoDB versione 3.x o successiva. SCRAM-SHA-1 Questi metodi di autenticazione vengono utilizzati per autenticare e crittografare le password MongoDB se gli utenti desiderano utilizzare le password per accedere ai database. L'autenticazione sugli AWS DMS endpoint garantisce che solo gli utenti autorizzati possano accedere e modificare i dati migrati tra i database. Senza un'autenticazione adeguata, gli utenti non autorizzati potrebbero essere in grado di accedere ai dati sensibili durante il processo di migrazione. Ciò può causare violazioni dei dati, perdita di dati o altri incidenti di sicurezza.

Correzione

Per abilitare un meccanismo di autenticazione sugli endpoint DMS per MongoDB, consulta Usare MongoDB come fonte nella Guida per l'utente. AWS DMSAWS Database Migration Service

[DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato

Requisiti correlati: NIST.800-53.r5 SC-8, PCI DSS NIST.800-53.r5 SC-13 v4.0. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::DMS::Endpoint`

Regola AWS Config : dms-redis-tls-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS DMS endpoint per Redis OSS è configurato con una connessione TLS. Il controllo fallisce se sull'endpoint non è abilitato TLS.

TLS offre una sicurezza end-to-end quando i dati vengono inviati tra applicazioni o database su Internet. Quando configuri la crittografia SSL per l'endpoint DMS, abilita la comunicazione crittografata tra i database di origine e di destinazione durante il processo di migrazione. Questo aiuta a prevenire l'intercettazione e l'intercettazione di dati sensibili da parte di malintenzionati. Senza la crittografia SSL, è possibile accedere ai dati sensibili, con conseguenti violazioni dei dati, perdita di dati o altri incidenti di sicurezza.

Correzione

Per abilitare una connessione TLS sugli endpoint DMS per Redis, consulta Using Redis come target nella Guida per l'utente. AWS Database Migration ServiceAWS Database Migration Service

[DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::DMS::ReplicationInstance`

Regola AWS Config : dms-replication-instance-multi-az-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istanza di replica AWS Database Migration Service (AWS DMS) è configurata per utilizzare più zone di disponibilità (Multi-AZ distribuzione). Il controllo ha esito negativo se l'istanza AWS DMS di replica non è configurata per utilizzare una Multi-AZ distribuzione.

In una Multi-AZ distribuzione, effettua AWS DMS automaticamente il provisioning e mantiene una replica in standby di un'istanza di replica in una zona di disponibilità (AZ) diversa. L'istanza di replica principale viene quindi replicata in modo sincrono nella replica in standby. Se l'istanza di replica primaria incorre in un guasto o non risponde, l'istanza di standby riprende tutte le attività in esecuzione con un'interruzione minima. Per ulteriori informazioni, consulta Lavorare con un'istanza di replica nella Guida per l'utente.AWS Database Migration Service

Correzione

Dopo aver creato un'istanza di AWS DMS replica, è possibile modificare le relative impostazioni Multi-AZ di distribuzione. Per informazioni sulla modifica di questa e di altre impostazioni per un'istanza di replica esistente, vedere Modifica di un'istanza di replica nella Guida per l'utente.AWS Database Migration Service

Controlli CSPM Security Hub per AWS DataSync

Questi controlli CSPM di Security Hub valutano il AWS DataSync servizio e le risorse. I controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[DataSync.1] DataSync le attività dovrebbero avere la registrazione abilitata

Requisiti correlati: CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::DataSync::Task`

Regola AWS Config : datasync-task-logging-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se per un' AWS DataSync attività è abilitata la registrazione. Il controllo fallisce se l'attività non ha la registrazione abilitata.

I registri di controllo tengono traccia e monitorano le attività del sistema. Forniscono una registrazione degli eventi che può aiutarvi a rilevare violazioni della sicurezza, indagare sugli incidenti e rispettare le normative. I registri di controllo migliorano anche la responsabilità e la trasparenza complessive dell'organizzazione.

Correzione

Per informazioni sulla configurazione della registrazione per le AWS DataSync attività, consulta Monitoraggio dei trasferimenti di dati con Amazon CloudWatch Logs nella Guida per l'AWS DataSync utente.

[DataSync.2] le DataSync attività devono essere etichettate

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::DataSync::Task`

Regola AWS Config : datasync-task-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un' AWS DataSync attività ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo ha esito negativo se l'attività non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'attività non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta creata e assegnata a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un' AWS DataSync attività, consulta Taggare le AWS DataSync attività nella Guida per l'AWS DataSync utente.

Controlli CSPM di Security Hub per Amazon Detective

Questo AWS Security Hub CSPM controllo valuta il servizio e le risorse di Amazon Detective. Il controllo potrebbe non essere disponibile in tuttiRegioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Detective.1] I grafici del comportamento dei Detective devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Detective::Graph`

AWS Configregola: `tagged-detective-graph` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	`No default value`

Questo controllo verifica se un grafico comportamentale di Amazon Detective contiene tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il grafico del comportamento non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo

verifica solo l'esistenza di una chiave di tag e fallisce se il grafico del comportamento non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un grafico del comportamento di un Detective, consulta Aggiungere tag a un grafico comportamentale nella Amazon Detective Administration Guide.

Controlli CSPM del Security Hub per Amazon DocumentDB

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse di Amazon DocumentDB (con compatibilità con MongoDB). I controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi

Requisiti correlati: 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), (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : docdb-cluster-encrypted

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon DocumentDB è crittografato a riposo. Il controllo fallisce se un cluster Amazon DocumentDB non è crittografato a riposo.

I dati inattivi si riferiscono a tutti i dati archiviati in uno storage persistente e non volatile per qualsiasi durata. La crittografia consente di proteggere la riservatezza di tali dati, riducendo il rischio che un utente non autorizzato possa accedervi. I dati nei cluster Amazon DocumentDB devono essere crittografati quando sono inattivi per un ulteriore livello di sicurezza. Amazon DocumentDB utilizza l'Advanced Encryption Standard a 256 bit (AES-256) per crittografare i dati utilizzando chiavi di crittografia archiviate in (). AWS Key Management Service AWS KMS

Correzione

Puoi abilitare la crittografia a riposo quando crei un cluster Amazon DocumentDB. Non è possibile modificare le impostazioni di crittografia dopo aver creato un cluster. Per ulteriori informazioni, consulta Enabling encryption at rest for an Amazon DocumentDB cluster nella Amazon DocumentDB Developer Guide.

[DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato

Requisiti correlati: PCI NIST.800-53.r5 SI-12 DSS v4.0. 1/3.2.1, Profilo CRI v2. 2/PR. DS-11.01

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : docdb-cluster-backup-retention-check

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`minimumBackupRetentionPeriod`	Periodo minimo di conservazione dei backup in giorni	Numero intero	Da 7 a 35	7	

Questo controllo verifica se un cluster Amazon DocumentDB ha un periodo di conservazione dei backup maggiore o uguale al periodo di tempo specificato. Il controllo fallisce se il periodo di conservazione del backup è inferiore al periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione del backup, Security Hub CSPM utilizza un valore predefinito di 7 giorni.

I backup aiutano a ripristinare più rapidamente un incidente di sicurezza e a rafforzare la resilienza dei sistemi. Automatizzando i backup per i cluster Amazon DocumentDB, sarai in grado di ripristinare i sistemi in un determinato momento e ridurre al minimo i tempi di inattività e la perdita di dati. In Amazon DocumentDB, i cluster hanno un periodo di conservazione dei backup predefinito di 1 giorno. Questo periodo deve essere aumentato a un valore compreso tra 7 e 35 giorni per passare questo controllo.

Correzione

Per modificare il periodo di conservazione dei backup per i cluster Amazon DocumentDB, consulta Modifying an Amazon DocumentDB cluster nella Amazon DocumentDB Developer Guide. Per Backup, scegli il periodo di conservazione del backup.

[DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche

Requisiti correlati: 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), (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, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: `AWS::RDS::DBClusterSnapshot`

Regola AWS Config : docdb-cluster-snapshot-public-prohibited

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se uno snapshot manuale del cluster di Amazon DocumentDB è pubblico. Il controllo fallisce se lo snapshot manuale del cluster è pubblico.

Uno snapshot manuale del cluster di Amazon DocumentDB non deve essere pubblico a meno che non sia previsto. Se condividi uno snapshot manuale non crittografato come pubblico, lo snapshot è disponibile per tutti. Account AWS Le istantanee pubbliche possono causare un'esposizione involontaria dei dati.

> **Note**
>
> Questo controllo valuta le istantanee manuali del cluster. Non puoi condividere uno snapshot del cluster automatizzato di Amazon DocumentDB. Tuttavia, puoi creare uno snapshot manuale copiando lo snapshot automatico e quindi condividerlo.

Correzione

Per rimuovere l'accesso pubblico agli snapshot manuali dei cluster di Amazon DocumentDB, consulta Sharing a snapshot nella Amazon DocumentDB Developer Guide. A livello di codice, puoi utilizzare l'operazione Amazon DocumentDB. `modify-db-snapshot-attribute` Imposta `attribute-name` come e come`restore`. `values-to-remove` `all`

[DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch

Requisiti correlati: 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), PCI NIST.800-53.r5 SI-7 DSS v4.0. 1/10.3.3, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-04.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : docdb-cluster-audit-logging-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon DocumentDB pubblica log di audit su Amazon Logs. CloudWatch Il controllo fallisce se il cluster non pubblica i log di controllo su Logs. CloudWatch

Amazon DocumentDB (con compatibilità con MongoDB) ti consente di controllare gli eventi che sono stati eseguiti nel tuo cluster. Sono esempi di eventi registrati i tentativi di autenticazione riusciti e non riusciti, l'eliminazione di una raccolta in un database o la creazione di un indice. Per impostazione predefinita, il controllo è disabilitato in Amazon DocumentDB e richiede l'intervento dell'utente per abilitarlo.

Correzione

Per pubblicare i log di audit di Amazon DocumentDB su CloudWatch Logs, consulta Enabling auditing nella Amazon DocumentDB Developer Guide.

[DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : docdb-cluster-deletion-protection-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon DocumentDB ha la protezione da eliminazione abilitata. Il controllo fallisce se nel cluster non è abilitata la protezione da eliminazione.

L'attivazione della protezione dall'eliminazione del cluster offre un ulteriore livello di protezione contro l'eliminazione accidentale del database o l'eliminazione da parte di un utente non autorizzato. Un cluster Amazon DocumentDB non può essere eliminato mentre la protezione da eliminazione è abilitata. È necessario innanzitutto disabilitare la protezione da eliminazione prima che una richiesta di eliminazione possa avere successo. La protezione da eliminazione è abilitata per impostazione predefinita quando crei un cluster nella console Amazon DocumentDB.

Correzione

Per abilitare la protezione da eliminazione per un cluster Amazon DocumentDB esistente, consulta Modifying an Amazon DocumentDB cluster nella Amazon DocumentDB Developer Guide. Nella sezione Modifica cluster, scegli Abilita la protezione da eliminazione.

[DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito

Requisiti correlati: CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : docdb-cluster-encrypted-in-transit

Tipo di pianificazione: periodica

Parametri:`excludeTlsParameters`:`disabled`, `enabled` (non personalizzabile)

Questo controllo verifica se un cluster Amazon DocumentDB richiede TLS per le connessioni al cluster. Il controllo fallisce se il gruppo di parametri del cluster associato al cluster non è sincronizzato o se il parametro del cluster TLS è impostato su o. `disabled` `enabled`

Puoi utilizzare TLS per crittografare la connessione tra un'applicazione e un cluster Amazon DocumentDB. L'uso di TLS può aiutare a proteggere i dati dall'intercettazione mentre sono in transito tra un'applicazione e un cluster Amazon DocumentDB. La crittografia in transito per un cluster Amazon DocumentDB viene gestita utilizzando il parametro TLS nel gruppo di parametri del cluster associato al cluster. Quando la crittografia in transito è abilitata, per connettersi al cluster sono necessarie connessioni protette tramite TLS. Consigliamo di utilizzare i seguenti parametri TLS:`tls1.2+`, `tls1.3+` e. `fips-140-3`

Correzione

Per informazioni sulla modifica delle impostazioni TLS per un cluster Amazon DocumentDB, consulta Encrypting data in transit nella Amazon DocumentDB Developer Guide.

Controlli CSPM del Security Hub per DynamoDB

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse di Amazon DynamoDB. I controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[DynamoDB.1] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda

Requisiti correlati: 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 Profile v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::DynamoDB::Table`

Regola AWS Config : `dynamodb-autoscaling-enabled`

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati validi	Valore predefinito CSPM di Security Hub
`minProvisionedReadCapacity`	Numero minimo di unità di capacità di lettura assegnate per la scalabilità automatica di DynamoDB	Numero intero	Da `1` a `40000`	Nessun valore predefinito
`targetReadUtilization`	Percentuale di utilizzo prevista per la capacità di lettura	Numero intero	Da `20` a `90`	Nessun valore predefinito
`minProvisionedWriteCapacity`	Numero minimo di unità di capacità di scrittura assegnate per la scalabilità automatica di DynamoDB	Numero intero	Da `1` a `40000`	Nessun valore predefinito
`targetWriteUtilization`	Percentuale di utilizzo prevista per la capacità di scrittura	Numero intero	Da `20` a `90`	Nessun valore predefinito

Questo controllo verifica se una tabella Amazon DynamoDB è in grado di scalare la propria capacità di lettura e scrittura in base alle esigenze. Il controllo fallisce se la tabella non utilizza la modalità di capacità su richiesta o la modalità provisioning con scalabilità automatica configurata. Per impostazione predefinita, questo controllo richiede solo la configurazione di una di queste modalità, indipendentemente da livelli specifici di capacità di lettura o scrittura. Facoltativamente, è possibile fornire valori di parametri personalizzati per richiedere livelli specifici di capacità di lettura e scrittura o di utilizzo del target.

La scalabilità della capacità in base alla domanda evita le eccezioni di limitazione, il che aiuta a mantenere la disponibilità delle applicazioni. Le tabelle DynamoDB che utilizzano la modalità di capacità su richiesta sono limitate solo dalle quote di tabella predefinite del throughput di DynamoDB. Per aumentare queste quote, puoi inviare un ticket di assistenza a. Supporto Le tabelle DynamoDB che utilizzano la modalità provisioning con scalabilità automatica regolano la capacità di throughput assegnata in modo dinamico in risposta ai modelli di traffico. Per ulteriori informazioni

sulla limitazione delle richieste di DynamoDB, consulta Request throttling and burst capacity nella Amazon DynamoDB Developer Guide.

Correzione

Per abilitare la scalabilità automatica di DynamoDB su tabelle esistenti in modalità capacità, consulta Enabling DynamoDB auto scaling su tabelle esistenti nella Amazon DynamoDB Developer Guide.

[DynamoDB.2] Le tabelle DynamoDB dovrebbero avere il ripristino point-in-time abilitato

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13 (5) NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-11.01

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: `AWS::DynamoDB::Table`

Regola AWS Config : `dynamodb-pitr-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il ripristino point-in-time (PITR) è abilitato per una tabella Amazon DynamoDB.

I backup ti aiutano a ripristinare più rapidamente un incidente di sicurezza. Inoltre, rafforzano la resilienza dei sistemi. Il ripristino point-in-time di DynamoDB automatizza i backup per le tabelle DynamoDB. Riduce i tempi di ripristino in seguito a operazioni di cancellazione o scrittura accidentali. Le tabelle DynamoDB con PITR abilitato possono essere ripristinate in qualsiasi momento negli ultimi 35 giorni.

Correzione

Per ripristinare una tabella DynamoDB in un momento specifico, consulta Restoring a DynamoDB table to a point-in-time nella Amazon DynamoDB Developer Guide.

[DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi

Requisiti correlati: 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), CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::DAX::Cluster`

Regola AWS Config : `dax-encryption-enabled`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un cluster Amazon DynamoDB Accelerator (DAX) è crittografato a riposo. Il controllo fallisce se il cluster DAX non è crittografato a riposo.

La crittografia dei dati inattivi riduce il rischio di accesso ai dati archiviati su disco da parte di un utente non autenticato. AWS La crittografia aggiunge un altro set di controlli di accesso per limitare la capacità degli utenti non autorizzati di accedere ai dati. Ad esempio, sono necessarie le autorizzazioni API per decrittografare i dati prima che possano essere letti.

Correzione

Non è possibile abilitare o disabilitare la crittografia a riposo dopo la creazione di un cluster. È necessario ricreare il cluster per abilitare la crittografia a riposo. Per istruzioni dettagliate su come creare un cluster DAX con la crittografia a riposo abilitata, consulta Enabling encryption at rest using the Console di gestione AWS nella Amazon DynamoDB Developer Guide.

[DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup

Requisiti correlati: 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-13 (5) NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-11.01

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: `AWS::DynamoDB::Table`

AWS Config regola: **`dynamodb-resources-protected-by-backup-plan`**

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`backupVaultLockCheck`	Il controllo restituisce un `PASSED` risultato se il parametro è impostato su `true` e la risorsa utilizza AWS Backup Vault Lock.	Booleano	`true` o `false`	Nessun valore predefinito

Questo controllo valuta se una `ACTIVE` tabella Amazon DynamoDB in stato è coperta da un piano di backup. Il controllo fallisce se la tabella DynamoDB non è coperta da un piano di backup. Se si imposta il `backupVaultLockCheck` parametro uguale a`true`, il controllo passa solo se viene eseguito il backup della tabella DynamoDB in AWS Backup un vault bloccato.

AWS Backup è un servizio di backup completamente gestito che consente di centralizzare e automatizzare il backup dei dati in tutto il mondo. Servizi AWS Con AWS Backup, è possibile creare piani di backup che definiscono i requisiti di backup, ad esempio la frequenza con cui eseguire il backup dei dati e per quanto tempo conservare tali backup. L'inclusione delle tabelle DynamoDB nei piani di backup consente di proteggere i dati da perdite o cancellazioni involontarie.

Correzione

Per aggiungere una tabella DynamoDB a AWS Backup un piano di backup, consulta Assegnazione di risorse a un piano di backup nella Developer Guide.AWS Backup

[DynamoDB.5] Le tabelle DynamoDB devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::DynamoDB::Table`

AWS Config regola: `tagged-dynamodb-table` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se una tabella Amazon DynamoDB contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la tabella non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la tabella non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una tabella DynamoDB, consulta Tagging resources in DynamoDB nella Amazon DynamoDB Developer Guide.

[DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata

Requisiti correlati: 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/GV. RM-01.03, Profilo CRI v2. 2/PR. DS-01.01

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: media

Tipo di risorsa: `AWS::DynamoDB::Table`

AWS Config regola: **`dynamodb-table-deletion-protection-enabled`**

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una tabella Amazon DynamoDB ha la protezione da eliminazione abilitata. Il controllo fallisce se una tabella DynamoDB non ha la protezione da eliminazione abilitata.

È possibile proteggere una tabella DynamoDB dall'eliminazione accidentale con la proprietà di protezione dall'eliminazione. L'attivazione di questa proprietà per le tabelle aiuta a garantire che le tabelle non vengano eliminate accidentalmente durante le normali operazioni di gestione delle tabelle da parte degli amministratori. Questo aiuta a prevenire interruzioni delle normali operazioni aziendali.

Correzione

Per abilitare la protezione da eliminazione per una tabella DynamoDB, consulta Using delete protection nella Amazon DynamoDB Developer Guide.

[DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito

Requisiti correlati: NIST.800-53.r5 AC-17,, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-13, PCI DSS NIST.800-53.r5 SC-23 v4.0. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::DAX::Cluster`

Regola AWS Config : `dax-tls-endpoint-encryption`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un cluster Amazon DynamoDB Accelerator (DAX) è crittografato in transito, con il tipo di crittografia degli endpoint impostato su TLS. Il controllo fallisce se il cluster DAX non è crittografato in transito.

Puoi utilizzare HTTPS (TLS) per impedire a potenziali aggressori di utilizzare attacchi di tipo person-in-the-middle o simili per intercettare o manipolare traffico di rete. È necessario consentire solo alle connessioni crittografate tramite TLS di accedere ai cluster DAX. Tuttavia, la crittografia dei dati in transito può influire sulle prestazioni. È consigliabile testare l'applicazione con la crittografia attivata per comprendere il profilo delle prestazioni e l'impatto del TLS.

Correzione

Non è possibile modificare l'impostazione di crittografia TLS dopo aver creato un cluster DAX. Per crittografare un cluster DAX esistente, crea un nuovo cluster con la crittografia in transito abilitata, trasferisci il traffico dell'applicazione su di esso, quindi elimina il vecchio cluster. Per ulteriori informazioni, consulta Uso della protezione da eliminazione nella Guida per gli sviluppatori di Amazon DynamoDB.

Controlli CSPM del Security Hub per Amazon EC2

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon Elastic Compute Cloud (Amazon EC2). I controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[EC2.1] Le istantanee di Amazon EBS non devono essere configurate per essere ripristinabili pubblicamente

Requisiti correlati: PCI DSS v3.2. 1/12.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 1/7.2.1, 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 Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `ebs-snapshot-public-restorable-check`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se gli snapshot di Amazon Elastic Block Store sono configurati per essere ripristinabili pubblicamente. Il controllo fallisce se gli snapshot di Amazon EBS sono configurati per essere ripristinabili da tutti.

Gli snapshot EBS vengono utilizzati per eseguire il backup dei dati sui volumi EBS su Amazon S3 in un momento specifico. Puoi utilizzare gli snapshot per ripristinare gli stati precedenti dei volumi EBS. Raramente è accettabile condividere uno snapshot con il pubblico. In genere la decisione di condividere pubblicamente uno snapshot viene presa per errore o senza una completa comprensione delle implicazioni. Questo controllo consente di garantire che tale condivisione sia stata completamente pianificata ed è intenzionale.

Correzione

Per rendere privata una snapshot EBS pubblica, consulta Share a snapshot nella Amazon EC2 User Guide. Per Azioni, Modifica le autorizzazioni, scegli Privato.

[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/5.5, PCI DSS v3.2. 1/1.2.1, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 1/2.1, benchmark AWS CIS Foundations v1.2. 0/4.3, benchmark AWS CIS Foundations v1.4. 0/5.3, benchmark AWS CIS Foundations v3.0. 0/5.4 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (11) 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), Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: `AWS::EC2::SecurityGroup`

Regola AWS Config : `vpc-default-security-group-closed`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il gruppo di sicurezza predefinito di un VPC consente il traffico in entrata o in uscita. Il controllo fallisce se il gruppo di sicurezza consente il traffico in entrata o in uscita.

Le regole per il gruppo di sicurezza predefinito consentono tutto il traffico in uscita e in ingresso dalle interfacce di rete (e le istanze associate) assegnate allo stesso gruppo di sicurezza. Ti consigliamo di non utilizzare il gruppo di sicurezza predefinito. Poiché il gruppo di sicurezza predefinito non può essere eliminato, è necessario modificare l'impostazione delle regole di gruppo di sicurezza predefinito per limitare il traffico in ingresso e in uscita. Ciò impedisce il traffico non intenzionale se il gruppo di sicurezza predefinito viene configurato accidentalmente per risorse come le istanze EC2.

Correzione

Per risolvere questo problema, inizia creando nuovi gruppi di sicurezza con privilegi minimi. Per istruzioni, consulta Creare un gruppo di sicurezza nella Amazon VPC User Guide. Quindi, assegna i nuovi gruppi di sicurezza alle tue istanze EC2. Per istruzioni, consulta Modificare il gruppo di sicurezza di un'istanza nella Guida per l'utente di Amazon EC2.

Dopo aver assegnato i nuovi gruppi di sicurezza alle tue risorse, rimuovi tutte le regole in entrata e in uscita dai gruppi di sicurezza predefiniti. Per istruzioni, consulta Configurare le regole dei gruppi di sicurezza nella Amazon VPC User Guide.

[EC2.3] I volumi Amazon EBS collegati devono essere crittografati quando sono inattivi

Requisiti correlati: 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), (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::EC2::Volume`

Regola AWS Config : `encrypted-volumes`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i volumi EBS che si trovano in uno stato collegato sono crittografati. Per superare questo controllo, i volumi EBS devono essere in uso e crittografati. Se il volume EBS non è collegato, non è destinato a questo controllo.

Per un ulteriore livello di sicurezza dei dati sensibili nei volumi EBS, è necessario abilitare la crittografia EBS dei dati inattivi. La crittografica Amazon EBS offre una soluzione di crittografia semplice per le risorse EBS che non richiede di creare, mantenere e proteggere la propria infrastruttura di gestione delle chiavi. Utilizza le chiavi KMS per la creazione di volumi e istantanee crittografati.

Per ulteriori informazioni sulla crittografia Amazon EBS, consulta Amazon EBS encryption nella Amazon EC2 User Guide.

Correzione

Non esiste un modo diretto per crittografare un volume o uno snapshot non crittografato esistente. È possibile crittografare un nuovo volume o snapshot solo quando viene creato.

Se hai abilitato la crittografia per impostazione predefinita, Amazon EBS crittografa il nuovo volume o snapshot risultante utilizzando la tua chiave predefinita per la crittografia Amazon EBS. Anche se non la crittografia non è abilitata per impostazione predefinita, è possibile abilitare la crittografia al momento della creazione di uno specifico volume o snapshot. In entrambi i casi, puoi sostituire la chiave predefinita per la crittografia Amazon EBS e scegliere una chiave simmetrica gestita dal cliente.

Per ulteriori informazioni, consulta Creare un volume Amazon EBS e Copiare uno snapshot Amazon EBS nella Guida per l'utente di Amazon EC2.

[EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato

Requisiti correlati: 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-08.01, Profilo CRI v2. 2/PR. PS-02.03

Categoria: Identificazione > Inventario

Gravità: media

Tipo di risorsa: `AWS::EC2::Instance`

AWS Config regola: `ec2-stopped-instance-days-check` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`AllowedDays`	Numero di giorni in cui l'istanza EC2 può rimanere in uno stato di arresto prima della generazione di un risultato non riuscito.	Numero intero	Da `1` a `365`	`30`

Questo controllo verifica se un'istanza Amazon EC2 è stata interrotta per un periodo superiore al numero di giorni consentito. Il controllo fallisce se un'istanza EC2 viene interrotta per un periodo di tempo superiore al periodo di tempo massimo consentito. A meno che non si fornisca un valore di parametro personalizzato per il periodo di tempo massimo consentito, Security Hub CSPM utilizza un valore predefinito di 30 giorni.

Quando un'istanza EC2 non viene eseguita per un periodo di tempo significativo, crea un rischio per la sicurezza perché l'istanza non viene gestita attivamente (analizzata, corretta, aggiornata).

Se viene avviata in un secondo momento, la mancanza di una manutenzione adeguata potrebbe causare problemi imprevisti nell'ambiente AWS . Per mantenere in modo sicuro un'istanza EC2 nel tempo in uno stato inattivo, avviala periodicamente per la manutenzione e poi interrompila dopo la manutenzione. Idealmente, questo dovrebbe essere un processo automatizzato.

> **Note**
>
> Questo controllo valuta il numero di giorni in cui un'istanza EC2 è stata interrotta utilizzando il timestamp di `StateTransitionReason` quell'istanza. Quando `StateTransitionReason` non include un timestamp (ad esempio quando un'istanza viene interrotta a causa di un errore interno), il controllo utilizza invece l'ora di avvio dell'istanza. In questo caso, se l'ora di avvio è precedente al periodo di tempo massimo consentito, il controllo genera un risultato NON RIUSCITO.

Correzione

Per terminare un'istanza EC2 inattiva, consulta Terminare un'istanza nella Amazon EC2 User Guide.

[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/3.7, benchmark AWS CIS Foundations v1.2. 0/2.9, benchmark AWS CIS Foundations v1.4. 0/3.9, benchmark AWS CIS Foundations v3.0. 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, 3.3.1, 3.13.1, PCI DSS versione NIST.800-171.r2 3.2. NIST.800-171.r2 1/10.3.3, PCI DSS versione 3.2. 1/10.3.4, PCI DSS versione 3.2. 1/10.3.5, PCI DSS versione 3.2. 1/10.3.6, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-04.02

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::EC2::VPC`

Regola AWS Config : `vpc-flow-logs-enabled`

Tipo di pianificazione: periodica

Parametri:

- `trafficType`: `REJECT` (non personalizzabile)

Questo controllo verifica se i log di flusso di Amazon VPC vengono trovati e abilitati per i VPC. Il tipo di traffico è impostato su. `Reject` Il controllo fallisce se i log di flusso VPC non sono abilitati per i VPC nel tuo account.

> **Note**
>
> Questo controllo non verifica se i log di flusso di Amazon VPC sono abilitati tramite Amazon Security Lake per. Account AWS

Con la funzione VPC Flow Logs, puoi acquisire informazioni sul traffico di indirizzi IP che va e viene dalle interfacce di rete nel tuo VPC. Dopo aver creato un log di flusso, puoi visualizzarne e recuperarne i dati in Logs. CloudWatch Per ridurre i costi, puoi anche inviare i log di flusso ad Amazon S3.

Security Hub CSPM consiglia di abilitare la registrazione del flusso per i pacchetti rifiutati per i VPC. I log di flusso forniscono visibilità sul traffico di rete che attraversa il VPC e possono rilevare traffico anomalo o fornire informazioni durante i flussi di lavoro di sicurezza.

Per impostazione predefinita, il record include i valori per i diversi componenti del flusso di indirizzi IP, tra cui origine, destinazione e protocollo. Per ulteriori informazioni e descrizioni dei campi di log, consulta VPC Flow Logs nella Amazon VPC User Guide.

Correzione

Per creare un log di flusso VPC, consulta Create a Flow Log nella Amazon VPC User Guide. Dopo aver aperto la console Amazon VPC, scegli I tuoi VPC. Per Filtro, scegli Rifiuta o Tutto.

[EC2.7] La crittografia predefinita di EBS deve essere abilitata

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/5.1.1, benchmark AWS CIS Foundations v1.4. 0/2.2.1, benchmark AWS CIS Foundations v3.0. 0/2.2.1, 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 (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `ec2-ebs-encryption-by-default`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la crittografia a livello di account è abilitata per impostazione predefinita per i volumi Amazon Elastic Block Store (Amazon EBS). Il controllo fallisce se la crittografia a livello di account non è abilitata per i volumi EBS.

Quando la crittografia è abilitata per il tuo account, i volumi Amazon EBS e le copie degli snapshot vengono crittografati quando sono inattivi. Ciò aggiunge un ulteriore livello di protezione per i tuoi dati. Per ulteriori informazioni, consulta la sezione Encryption by default nella Guida per l'utente di Amazon EC2.

Correzione

Per configurare la crittografia predefinita per i volumi Amazon EBS, consulta Encryption by default nella Amazon EC2 User Guide.

[EC2.8] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/5.7, benchmark AWS CIS Foundations v3.0. 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 versione 4.0. 1/2.2.6, Profilo CRI v2. 2/PR. AA-04.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Sicurezza di rete

Gravità: alta

Tipo di risorsa: `AWS::EC2::Instance`

Regola AWS Config : `ec2-imdsv2-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la versione dei metadati dell'istanza EC2 è configurata con Instance Metadata Service versione 2 (IMDSv2). Il controllo passa se `HttpTokens` è impostato su obbligatorio per IMDSv2. Il controllo ha esito negativo se `HttpTokens` è impostato su. `optional`

I metadati dell'istanza vengono utilizzati per configurare o gestire l'istanza in esecuzione. L'IMDS fornisce l'accesso a credenziali temporanee, che vengono ruotate frequentemente. Queste credenziali eliminano la necessità di codificare o distribuire credenziali riservate alle istanze manualmente o programmaticamente. L'IMDS è collegato localmente a ogni istanza EC2. Funziona su uno speciale indirizzo IP «link local» 169.254.169.254. Questo indirizzo IP è accessibile solo dal software in esecuzione sull'istanza.

La versione 2 dell'IMDS aggiunge nuove protezioni per i seguenti tipi di vulnerabilità. Queste vulnerabilità potrebbero essere utilizzate per tentare di accedere all'IMDS.

- Apri i firewall delle applicazioni del sito Web
- Apri proxy inversi
- Server-side vulnerabilità relative alla contraffazione della richiesta (SSRF)
- Firewall Open Layer 3 e NAT (Network Address Translation)

Security Hub CSPM consiglia di configurare le istanze EC2 con IMDSv2.

Correzione

Per configurare le istanze EC2 con IMDSv2, consulta Percorso consigliato per richiedere IMDSv2 nella Amazon EC2 User Guide.

[EC2.9] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico

Requisiti correlati: 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 Profile v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.02, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::EC2::Instance`

Regola AWS Config : `ec2-instance-no-public-ip`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le istanze EC2 hanno un indirizzo IP pubblico. Il controllo fallisce se il `publicIp` campo è presente nell'elemento di configurazione dell'istanza EC2. Questo controllo si applica solo agli indirizzi IPv4.

Un indirizzo IPv4 pubblico è un indirizzo IP raggiungibile da Internet. Se avvii l'istanza con un indirizzo IP pubblico, l'istanza EC2 è raggiungibile da Internet. Un indirizzo IPv4 privato è un indirizzo IP non raggiungibile da Internet. Puoi utilizzare indirizzi IPv4 privati per la comunicazione tra istanze EC2 nello stesso VPC o nella tua rete privata connessa.

Gli indirizzi IPv6 sono unici a livello globale e quindi sono raggiungibili da Internet. Tuttavia, per impostazione predefinita, tutte le sottoreti hanno l'attributo di indirizzamento IPv6 impostato su false. Per ulteriori informazioni su IPv6, consulta la sezione Indirizzamento IP nel tuo VPC nella Amazon VPC User Guide.

Se hai un caso d'uso legittimo per mantenere istanze EC2 con indirizzi IP pubblici, puoi eliminare i risultati di questo controllo. Per ulteriori informazioni sulle opzioni di architettura front-end, consulta l'AWS Architecture Blog o la serie di video della serie This Is My Architecture. AWS

Correzione

Utilizza un VPC non predefinito in modo che all'istanza non venga assegnato un indirizzo IP pubblico per impostazione predefinita.

Quando avvii un'istanza EC2 in un VPC predefinito, a essa viene assegnato un indirizzo IP pubblico. Quando avvii un'istanza EC2 in un VPC non predefinito, la configurazione della sottorete determina se riceve un indirizzo IP pubblico. La sottorete dispone di un attributo per determinare se le nuove istanze EC2 nella sottorete ricevono un indirizzo IP pubblico dal pool di indirizzi IPv4 pubblico.

Puoi dissociare un indirizzo IP pubblico assegnato automaticamente dalla tua istanza EC2. Per ulteriori informazioni, consulta Indirizzi IPv4 pubblici e nomi host DNS esterni nella Guida dell'utente di Amazon EC2.

[EC2.10] Amazon EC2 deve essere configurato per utilizzare gli endpoint VPC creati per il servizio Amazon EC2

Requisiti correlati: 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), (3), NIST.800-53.r5

SC-7 NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.3, 3.13.1, CRI Profile v2. NIST.800-171.r2 2/PR. AA-03.02, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Configurazione di rete sicura > Accesso privato alle API

Gravità: media

Tipo di risorsa: `AWS::EC2::VPC`

Regola AWS Config : vpc-endpoint-enabled

Tipo di pianificazione: periodica

Parametri:

- `serviceNames`: `ec2` (non personalizzabile)

Questo controllo verifica se viene creato un endpoint di servizio per Amazon EC2 per ogni VPC. Il controllo fallisce se un VPC non dispone di un endpoint VPC creato per il servizio Amazon EC2.

Questo controllo valuta le risorse in un unico account. Non può descrivere risorse esterne all'account. Poiché AWS Config Security Hub CSPM non effettua controlli tra account, verranno visualizzati `FAILED` i risultati relativi ai VPC condivisi tra account. Security Hub CSPM consiglia di eliminare questi risultati. `FAILED`

Per migliorare il livello di sicurezza del tuo VPC, puoi configurare Amazon EC2 per utilizzare un endpoint VPC di interfaccia. Gli endpoint di interfaccia sono basati su una tecnologia che consente di accedere alle operazioni delle API di Amazon EC2 in modo privato. AWS PrivateLink Limita tutto il traffico di rete tra il tuo VPC e Amazon EC2 alla rete Amazon. Poiché gli endpoint sono supportati solo all'interno della stessa regione, non è possibile creare un endpoint tra un VPC e un servizio in una regione diversa. In questo modo si evitano chiamate involontarie all'API Amazon EC2 verso altre regioni.

Per ulteriori informazioni sulla creazione di endpoint VPC per Amazon EC2, consulta Amazon EC2 e interfaccia gli endpoint VPC nella Amazon EC2 User Guide.

Correzione

Per creare un endpoint di interfaccia verso Amazon EC2 dalla console Amazon VPC, consulta Creare un endpoint VPC nella Guida.AWS PrivateLink Per il nome del servizio, scegli com.amazonaws. ***region***.ec2.

Puoi anche creare e allegare una policy per gli endpoint al tuo endpoint VPC per controllare l'accesso all'API Amazon EC2. Per istruzioni sulla creazione di una policy per gli endpoint VPC, consulta Create an endpoint policy nella Amazon EC2 User Guide.

[EC2.12] Gli EIP Amazon EC2 non utilizzati devono essere rimossi

Requisiti correlati: PCI DSS v3.2. 1/2.4, NIST.800-53.r5 CM-8 (1), Profilo CRI v2. 2/ID. AM-08.01, Profilo CRI v2. 2/ID. AM-08.02

Categoria: Protezione > Configurazione di rete protetta

Gravità: bassa

Tipo di risorsa: `AWS::EC2::EIP`

Regola AWS Config : `eip-attached`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se gli indirizzi IP elastici (EIP) allocati a un VPC sono collegati a istanze EC2 o interfacce di rete elastiche (ENI) in uso.

Un risultato non riuscito indica che potresti avere EIP EC2 inutilizzati.

Ciò ti aiuterà a mantenere un inventario accurato degli asset EIP nel tuo ambiente di dati dei titolari di carta (CDE).

Correzione

Per rilasciare un EIP inutilizzato, consulta Release an Elastic IP address nella Amazon EC2 User Guide.

[EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/4.1 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, (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), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.3, 3.13.1, PCI DSS versione NIST.800-171.r2 3.2. 1/1.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/2.2.2, PCI DSS versione 4.0. 1/1.3.1, Profilo CRI v2.

2/PR. AA-03.02, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. IR-01.05, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: `AWS::EC2::SecurityGroup`

Regola AWS Config : `restricted-ssh`

Tipo di pianificazione: modifica attivata e periodica

Parametri: nessuno

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 consente l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22. Il controllo fallisce se il gruppo di sicurezza consente l'ingresso da 0.0.0. 0/0oppure: :/0 alla porta 22.

I gruppi di sicurezza forniscono filtraggio stateful del traffico di rete in entrata e in uscita a risorse AWS . È opportuno che nessun gruppo di sicurezza consenta accesso di entratata illimitato alla porta 22. La rimozione di connettività senza alcuna restrizione a servizi della console remota, ad esempio SSH, riduce l'esposizione di un server ai rischi.

Correzione

Per vietare l'accesso alla porta 22, rimuovi la regola che consente tale accesso per ogni gruppo di sicurezza associato a un VPC. Per istruzioni, consulta Aggiornare le regole dei gruppi di sicurezza nella Guida per l'utente di Amazon EC2. Dopo aver selezionato un gruppo di sicurezza nella console Amazon EC2, scegli Azioni, Modifica regole in entrata. Rimuovi la regola che consente l'accesso alla porta 22.

[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/4.2, PCI DSS versione 4.0. 1/1.3.1, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: `AWS::EC2::SecurityGroup`

AWS Config regola: **`restricted-common-ports`**(la regola creata è`restricted-rdp`)

Tipo di pianificazione: modifica attivata e periodica

Parametri: nessuno

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 consente l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389. Il controllo fallisce se il gruppo di sicurezza consente l'ingresso da 0.0.0. 0/0oppure: :/0 alla porta 3389.

I gruppi di sicurezza forniscono filtraggio stateful del traffico di rete in entrata e in uscita a risorse AWS . È opportuno che nessun gruppo di sicurezza consenta accesso di entrata illimitato alla porta 3389. La rimozione di connettività senza alcuna restrizione a servizi della console remota, ad esempio RDP, riduce l'esposizione di un server ai rischi.

Correzione

Per vietare l'accesso alla porta 3389, rimuovi la regola che consente tale accesso per ogni gruppo di sicurezza associato a un VPC. Per istruzioni, consulta Aggiornare le regole dei gruppi di sicurezza nella Amazon VPC User Guide. Dopo aver selezionato un gruppo di sicurezza nella console Amazon VPC, scegli Azioni, Modifica regole in entrata. Rimuovi la regola che consente l'accesso alla porta 3389.

[EC2.15] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici

Requisiti correlati: 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), PCI DSS v4.0. 1/1.4.4, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Sicurezza di rete

Gravità: media

Tipo di risorsa: `AWS::EC2::Subnet`

Regola AWS Config : `subnet-auto-assign-public-ip-disabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una sottorete Amazon Virtual Private Cloud (Amazon VPC) è configurata per l'assegnazione automatica di indirizzi IP pubblici. Il controllo fallisce se la sottorete è configurata per l'assegnazione automatica di indirizzi IPv4 o IPv6 pubblici.

Le sottoreti dispongono di attributi che determinano se le interfacce di rete ricevono automaticamente indirizzi IPv4 e IPv6 pubblici. Per IPv4, questo attributo è impostato su per le sottoreti predefinite e `TRUE` `FALSE` per le sottoreti non predefinite (ad eccezione delle sottoreti non predefinite create tramite la procedura guidata di avvio dell'istanza EC2, dove è impostato su). `TRUE` Per IPv6, questo attributo è impostato su tutte le sottoreti per impostazione predefinita. `FALSE` Quando questi attributi sono abilitati, le istanze avviate nella sottorete ricevono automaticamente gli indirizzi IP corrispondenti (IPv4 o IPv6) sulla loro interfaccia di rete principale.

Correzione

Per configurare una sottorete in modo che non assegni indirizzi IP pubblici, consulta Modificare gli attributi di indirizzo IP della sottorete nella Amazon VPC User Guide.

[EC2.16] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse

Requisiti correlati: NIST.800-53.r5 CM-8 (1), NIST.800-171.r2 3.4.7, PCI DSS v4.0. 1/1.2.7, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Sicurezza di rete

Gravità: bassa

Tipo di risorsa: `AWS::EC2::NetworkAcl`

Regola AWS Config : `vpc-network-acl-unused-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se ci sono elenchi di controllo degli accessi alla rete (ACL di rete) non utilizzati nel tuo cloud privato virtuale (VPC). Il controllo fallisce se l'ACL di rete non è associato a una sottorete. Il controllo non genera risultati per un ACL di rete predefinito non utilizzato.

Il controllo verifica la configurazione degli elementi della risorsa `AWS::EC2::NetworkAcl` e determina le relazioni dell'ACL di rete.

Se l'unica relazione è il VPC dell'ACL di rete, il controllo fallisce.

Se sono elencate altre relazioni, il controllo passa.

Correzione

Per istruzioni sull'eliminazione di un ACL di rete non utilizzato, consulta Eliminazione di un ACL di rete nella Amazon VPC User Guide. Non puoi eliminare l'ACL di rete predefinito o un ACL associato alle sottoreti.

[EC2.17] Le istanze Amazon EC2 non devono utilizzare più ENI

Requisiti correlati: NIST.800-53.r5 AC-4 (21), CRI Profile v2. 2/PR. PS-01.02

Categoria: Protezione > Sicurezza di rete

Gravità: bassa

Tipo di risorsa: `AWS::EC2::Instance`

Regola AWS Config : `ec2-instance-multiple-eni-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istanza EC2 utilizza più Elastic Network Interface (ENI) o Elastic Fabric Adapters (EFA). Questo controllo passa se viene utilizzata una singola scheda di rete. Il controllo include un elenco di parametri opzionale per identificare gli ENI consentiti. Questo controllo fallisce anche se un'istanza EC2 appartenente a un cluster Amazon EKS utilizza più di un ENI. Se le tue istanze EC2 devono avere più ENI come parte di un cluster Amazon EKS, puoi eliminare tali risultati di controllo.

Più ENI possono causare istanze dual-homed, ossia istanze con più sottoreti. Ciò può aumentare la complessità della sicurezza della rete e introdurre percorsi e accessi di rete indesiderati.

Correzione

Per scollegare un'interfaccia di rete da un'istanza EC2, consulta Scollegare un'interfaccia di rete da un'istanza nella Amazon EC2 User Guide.

[EC2.18] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate

Requisiti correlati: 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), (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, 3.13.1, CRI Profile v2. NIST.800-171.r2 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Configurazione di rete sicura > Configurazione del gruppo di sicurezza

Gravità: alta

Tipo di risorsa: `AWS::EC2::SecurityGroup`

Regola AWS Config : `vpc-sg-open-only-to-authorized-ports`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`authorizedTcpPorts`	Elenco delle porte TCP autorizzate	IntegerList (minimo 1 elemento e massimo 32 elementi)	Da 1 a 65535	`[80,443]`
`authorizedUdpPorts`	Elenco delle porte UDP autorizzate	IntegerList (minimo 1 articolo e massimo 32 articoli)	Da 1 a 65535	Nessun valore predefinito

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 consente il traffico in entrata senza restrizioni da porte non autorizzate. Lo stato del controllo è determinato come segue:

- Se si utilizza il valore predefinito per`authorizedTcpPorts`, il controllo ha esito negativo se il gruppo di sicurezza consente il traffico in entrata senza restrizioni da qualsiasi porta diversa dalle porte 80 e 443.
- Se fornisci valori personalizzati per `authorizedTcpPorts` o`authorizedUdpPorts`, il controllo ha esito negativo se il gruppo di sicurezza consente il traffico in entrata senza restrizioni da qualsiasi porta non elencata.

I gruppi di sicurezza forniscono un filtraggio statico del traffico di rete in ingresso e in uscita verso. AWS Le regole dei gruppi di sicurezza devono seguire il principio dell'accesso con privilegi minimi. L'accesso illimitato (indirizzo IP con suffisso /0) aumenta la possibilità di attività dannose come pirateria informatica, attacchi denial-of-service e perdita di dati. A meno che una porta non sia espressamente consentita, la porta dovrebbe negare l'accesso illimitato.

Correzione

Per modificare un gruppo di sicurezza, consulta Work with security groups nella Amazon VPC User Guide.

[EC2.19] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio

Requisiti correlati: 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, NIST.800-53.r5 CM-2 (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, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Accesso limitato alla rete

Severità: critica

Tipo di risorsa: `AWS::EC2::SecurityGroup`

AWS Config regola: **`restricted-common-ports`**(la regola creata è`vpc-sg-restricted-common-ports`)

Tipo di pianificazione: modifica attivata e periodica

Parametri: `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` (non personalizzabile)

Questo controllo verifica se il traffico in entrata senza restrizioni per un gruppo di sicurezza Amazon EC2 è accessibile alle porte specificate considerate ad alto rischio. Questo controllo ha esito negativo se una delle regole di un gruppo di sicurezza consente il traffico in ingresso da '0.0.0. 0/0' o ': :/0' verso quelle porte.

I gruppi di sicurezza forniscono filtraggio stateful del traffico di rete in entrata e in uscita a risorse AWS . Accesso illimitato (0.0.0. 0/0) aumenta le opportunità di attività dannose, come la pirateria informatica, gli attacchi denial-of-service e la perdita di dati. Nessun gruppo di sicurezza dovrebbe consentire l'accesso illimitato in ingresso alle seguenti porte:

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIF)
- 1433, 1434 (SQL)
- 3000 (framework di sviluppo web Node.js Go e Ruby)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (framework di sviluppo web in Python)
- 5432 (postgresql)
- 5500 (fcp-addr-srvr1)
- 5601 (OpenSearch Cruscotti)
- 8080 (proxy)
- 8088 (porta HTTP precedente)
- 8888 (porta HTTP alternativa)
- 9200 o 9300 () OpenSearch

Correzione

Per eliminare le regole da un gruppo di sicurezza, consulta Eliminare le regole da un gruppo di sicurezza nella Guida per l'utente di Amazon EC2.

[EC2.20] Entrambi i tunnel VPN per un AWS Site-to-Site La connessione VPN dovrebbe essere attiva

Requisiti correlati: 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), NIST.800-171.r2 3.1.13, NIST.800-171.r2 3.1.20, CRI Profile v2. 2/GV. RM-09.02, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::EC2::VPNConnection`

Regola AWS Config : `vpc-vpn-2-tunnels-up`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Un tunnel VPN è un collegamento crittografato in cui i dati possono passare dalla rete del cliente a o dall' AWS interno di una connessione AWS Site-to-Site VPN. Ogni connessione VPN include due tunnel VPN che è possibile utilizzare contemporaneamente per una disponibilità elevata. Garantire che entrambi i tunnel VPN siano attivi per una connessione VPN è importante per confermare una connessione sicura e ad alta disponibilità tra un AWS VPC e la rete remota.

Questo controllo verifica che entrambi i tunnel VPN forniti dalla AWS Site-to-Site VPN abbiano lo stato UP. Il controllo fallisce se uno o entrambi i tunnel sono in stato INATTIVO.

Correzione

Per modificare le opzioni del tunnel VPN, consulta Modificare le opzioni del tunnel Site-to-Site VPN nella Guida per l'utente AWS Site-to-Site VPN.

[EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/5.2, benchmark AWS CIS Foundations v1.4. 0/5.1, benchmark AWS CIS Foundations v3.0. 0/5.1, NIST.800-53.r5 AC-4 (21), (1),

NIST.800-53.r5 CA-9 (2), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (21), NIST.800-53.r5 SC-7 (5) NIST.800-53.r5 CM-7 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, 3.13.1, PCI DSS versione 4.0. NIST.800-171.r2 1/1.3.1, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-01.05

Categoria: Protezione > Configurazione di rete sicura

Gravità: media

Tipo di risorsa: `AWS::EC2::NetworkAcl`

Regola AWS Config : `nacl-no-unrestricted-ssh-rdp`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una lista di controllo degli accessi alla rete (Network ACL) consente l'accesso illimitato alle porte TCP predefinite per il traffico in ingresso. SSH/RDP Il controllo fallisce se la voce ACL di rete in ingresso consente un blocco CIDR di origine di '0.0.0. 0/0' o ': :/0' per le porte TCP 22 o 3389. Il controllo non genera risultati per un ACL di rete predefinito.

L'accesso alle porte di amministrazione del server remoto, come la porta 22 (SSH) e la porta 3389 (RDP), non dovrebbe essere accessibile al pubblico, in quanto ciò potrebbe consentire l'accesso non intenzionale alle risorse all'interno del tuo VPC.

Correzione

Per modificare le regole del traffico ACL di rete, consulta Lavora con gli ACL di rete nella Amazon VPC User Guide.

[EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi

Requisiti correlati: CRI Profile v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02

Categoria: Identificazione > Inventario

Gravità: media

Tipo di risorsa:`AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`

Regola AWS Config : `ec2-security-group-attached-to-eni-periodic`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se i gruppi di sicurezza sono collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a un'interfaccia di rete elastica. Il controllo fallisce se il gruppo di sicurezza non è associato a un'istanza Amazon EC2 o a un'interfaccia di rete elastica.

> **Important**
>
> Il 20 settembre 2023, Security Hub CSPM ha rimosso questo controllo dagli standard AWS Foundational Security Best Practices e NIST SP 800-53 Revision 5. Questo controllo continua a far parte dello standard di gestione dei servizi. AWS Control Tower Questo controllo produce un risultato positivo se i gruppi di sicurezza sono collegati a istanze EC2 o a un'interfaccia di rete elastica. Tuttavia, in alcuni casi d'uso, i gruppi di sicurezza non collegati non rappresentano un rischio per la sicurezza. Puoi utilizzare altri controlli EC2 EC2.2, come,, EC2.13 EC2.14, e EC2.19 —per monitorare i tuoi EC2.18 gruppi di sicurezza.

Correzione

Per creare, assegnare ed eliminare gruppi di sicurezza, consulta la sezione Gruppi di sicurezza per le istanze EC2 nella Amazon EC2 User Guide.

[EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC

Requisiti correlati: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: `AWS::EC2::TransitGateway`

Regola AWS Config : `ec2-transit-gateway-auto-vpc-attach-disabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i gateway di transito EC2 accettano automaticamente allegati VPC condivisi. Questo controllo non riesce per un gateway di transito che accetta automaticamente richieste di allegati VPC condivise.

L'attivazione `AutoAcceptSharedAttachments` configura un gateway di transito per accettare automaticamente qualsiasi richiesta di allegati VPC tra account senza verificare la richiesta o l'account da cui proviene l'allegato. Per seguire le migliori pratiche di autorizzazione e autenticazione, consigliamo di disattivare questa funzionalità per garantire che vengano accettate solo le richieste di allegati VPC autorizzate.

Correzione

Per modificare un gateway di transito, consulta Modificare un gateway di transito nella Amazon VPC Developer Guide.

[EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati

Requisiti correlati: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), CRI Profile v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-02.03

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: `AWS::EC2::Instance`

Regola AWS Config : `ec2-paravirtual-instance-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il tipo di virtualizzazione di un'istanza EC2 è paravirtuale. Il controllo fallisce se l'istanza EC2 è `virtualizationType` impostata su. `paravirtual`

Le Amazon Machine Images (AMI) Linux utilizzano uno dei due tipi di virtualizzazione: paravirtual (PV) o hardware virtual machine (HVM). Le principali differenze tra le AMI PV e HVM risiedono nel

modo in cui vengono avviate e nella loro capacità di sfruttare i vantaggi delle estensioni hardware speciali (CPU, rete e archiviazione) per l'ottimizzazione delle prestazioni.

Storicamente parlando, i sistemi guest PV sono caratterizzati da prestazioni migliori rispetto ai sistemi guest HVM in molti casi, ma in seguito ai miglioramenti apportati alla virtualizzazione HVM e alla disponibilità di driver PV per AMI HVM, ciò non è più vero. Per ulteriori informazioni, consulta i tipi di virtualizzazione delle AMI Linux nella Guida per l'utente di Amazon EC2.

Correzione

Per aggiornare un'istanza EC2 a un nuovo tipo di istanza, consulta Cambia il tipo di istanza nella Amazon EC2 User Guide.

[EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::EC2::LaunchTemplate`

Regola AWS Config : `ec2-launch-template-public-ip-disabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i modelli di lancio di Amazon EC2 sono configurati per assegnare indirizzi IP pubblici alle interfacce di rete al momento dell'avvio. Il controllo fallisce se un modello di avvio EC2 è configurato per assegnare un indirizzo IP pubblico alle interfacce di rete.

Un indirizzo IP pubblico è raggiungibile da Internet. Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete potrebbero essere raggiungibili da Internet. Le risorse EC2 non dovrebbero essere accessibili al pubblico perché ciò potrebbe consentire l'accesso involontario ai tuoi carichi di lavoro.

Correzione

Per aggiornare un modello di lancio EC2, consulta Modifica delle impostazioni dell'interfaccia di rete predefinita nella Amazon EC2 Auto Scaling User Guide.

[EC2.28] I volumi EBS devono essere coperti da un piano di backup

Categoria: Recover > Resilience > Backup abilitati

Requisiti correlati: 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 SC-5 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13 (5) NIST.800-53.r5 SI-12, CRI Profile v2. 2/GV. RM-09.02, Profilo CRI v2. 2/PR. DS-01.02, Profilo CRI v2. 2/PR. DS-11.01, Profilo CRI v2. 2/PR. IR-03.01

Gravità: bassa

Tipo di risorsa: `AWS::EC2::Volume`

AWS Config regola: **`ebs-resources-protected-by-backup-plan`**

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`backupVaultLockCheck`	Il controllo restituisce un `PASSED` risultato se il parametro è impostato su `true` e la risorsa utilizza AWS Backup Vault Lock.	Booleano	`true` o `false`	Nessun valore predefinito

Questo controllo valuta se un volume Amazon EBS in `in-use` stato è coperto da un piano di backup. Il controllo fallisce se un volume EBS non è coperto da un piano di backup. Se si imposta il `backupVaultLockCheck` parametro uguale `a``true`, il controllo passa solo se viene eseguito il backup del volume EBS in un vault AWS Backup bloccato.

I backup consentono di ripristinare più rapidamente un incidente di sicurezza. Inoltre, rafforzano la resilienza dei sistemi. L'inclusione dei volumi Amazon EBS in un piano di backup aiuta a proteggere i dati da perdite o eliminazioni involontarie.

Correzione

Per aggiungere un volume Amazon EBS a un piano di AWS Backup backup, consulta Assegnazione di risorse a un piano di backup nella AWS Backup Developer Guide.

[EC2.33] Gli allegati del gateway di transito EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::TransitGatewayAttachment`

AWS Config regola: `tagged-ec2-transitgatewayattachment` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un allegato del gateway di transito Amazon EC2 ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo ha esito negativo se l'allegato Transit Gateway non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se l'allegato del gateway di transito non è

etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un allegato del gateway di transito EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::TransitGatewayRouteTable`

AWS Config regola: `tagged-ec2-transitgatewayroutetable` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se una tabella di routing del gateway di transito Amazon EC2 contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo ha esito negativo se la tabella delle rotte del gateway di transito non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la tabella di route del gateway di transito non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una tabella di routing del gateway di transito EC2, consulta Etichettare le risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.35] Le interfacce di rete EC2 devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::NetworkInterface`

AWS Config regola: `tagged-ec2-networkinterface` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un'interfaccia di rete Amazon EC2 ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'interfaccia di rete non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'interfaccia di rete non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'interfaccia di rete EC2, consulta Etichettare le risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.36] I gateway per i clienti EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::CustomerGateway`

AWS Config regola: `tagged-ec2-customergateway` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un gateway per clienti Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gateway del cliente non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gateway del cliente non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gateway clienti EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.37] Gli indirizzi IP elastici EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::EIP`

AWS Config regola: `tagged-ec2-eip` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un indirizzo IP elastico di Amazon EC2 ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'indirizzo IP elastico non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'indirizzo IP elastico non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un indirizzo IP elastico EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.38] Le istanze EC2 devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::Instance`

AWS Config regola: `tagged-ec2-instance` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un'istanza Amazon EC2 ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'istanza non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'istanza non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'istanza EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.39] I gateway Internet EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::InternetGateway`

AWS Config regola: `tagged-ec2-internetgateway` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un gateway Internet Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gateway Internet non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se il gateway Internet non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gateway Internet EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.40] I gateway NAT EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::NatGateway`

AWS Config regola: `tagged-ec2-natgateway` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un gateway NAT (Network Address Translation) di Amazon EC2 ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gateway NAT non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gateway NAT non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gateway NAT EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.41] Gli ACL di rete EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::NetworkAcl`

AWS Config regola: `tagged-ec2-networkacl` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se una lista di controllo degli accessi alla rete di Amazon EC2 (Network ACL) contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'ACL di rete non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'ACL di rete non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un ACL di rete EC2, consulta Etichettare le risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.42] Le tabelle delle rotte EC2 devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::RouteTable`

AWS Config regola: `tagged-ec2-routetable` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se una tabella di routing di Amazon EC2 contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la tabella di routing non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la tabella delle rotte non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una tabella di routing EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.43] I gruppi di sicurezza EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::SecurityGroup`

AWS Config regola: `tagged-ec2-securitygroup` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gruppo di sicurezza non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di sicurezza non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gruppo di sicurezza EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.44] Le sottoreti EC2 devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::Subnet`

AWS Config regola: `tagged-ec2-subnet` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se una sottorete Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la sottorete non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la sottorete non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una sottorete EC2, consulta Tagga le risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.45] I volumi EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::Volume`

AWS Config regola: `tagged-ec2-volume` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un volume Amazon EC2 ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il volume non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il volume non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un volume EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.46] I VPC Amazon devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::VPC`

AWS Config regola: `tagged-ec2-vpc` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un Amazon Virtual Private Cloud (Amazon VPC) ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se Amazon VPC non dispone di chiavi di tag o se non dispone di tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se Amazon VPC non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un VPC, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.47] I servizi endpoint Amazon VPC devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::VPCEndpointService`

AWS Config regola: `tagged-ec2-vpcendpointservice` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un servizio endpoint Amazon VPC dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il servizio endpoint non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il servizio endpoint non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un servizio endpoint Amazon VPC, consulta Manage Tags nella sezione Configura un servizio endpoint della Guida.AWS PrivateLink

[EC2.48] I log di flusso di Amazon VPC devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::FlowLog`

AWS Config regola: `tagged-ec2-flowlog` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un log di flusso Amazon VPC contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il log di flusso non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il log di flusso non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un log di flusso di Amazon VPC, consulta Etichettare un log di flusso nella Amazon VPC User Guide.

[EC2.49] Le connessioni peering Amazon VPC devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::VPCPeeringConnection`

AWS Config regola: `tagged-ec2-vpcpeeringconnection` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se una connessione peering Amazon VPC ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la connessione peering non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la connessione peering non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una connessione peering Amazon VPC, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.50] I gateway VPN EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::VPNGateway`

AWS Config regola: `tagged-ec2-vpngateway` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un gateway VPN Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gateway VPN non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se il gateway VPN non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gateway VPN EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata

Requisiti correlati: 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), (20), NIST.800-53.r5 SI-3 (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 v4.0 NIST.800-171.r2 . 1/10.2.1, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: bassa

Tipo di risorsa: `AWS::EC2::ClientVpnEndpoint`

AWS Config regola: **`ec2-client-vpn-connection-log-enabled`**

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS Client VPN endpoint ha abilitato la registrazione delle connessioni client. Il controllo fallisce se sull'endpoint non è abilitata la registrazione delle connessioni client.

Gli endpoint Client VPN consentono ai client remoti di connettersi in modo sicuro alle risorse in un Virtual Private Cloud (VPC) in. AWS I log di connessione consentono di tracciare l'attività degli utenti sull'endpoint VPN e forniscono visibilità. Quando attivi la registrazione delle connessioni, puoi specificare il nome di un flusso di log nel gruppo di log. Se non specifichi un flusso di log, il servizio Client VPN ne crea uno per te.

Correzione

Per abilitare la registrazione delle connessioni, consulta Abilitare la registrazione della connessione per un endpoint Client VPN esistente nella Guida per l'AWS Client VPN amministratore.

[EC2.52] I gateway di transito EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::TransitGateway`

AWS Config regola: `tagged-ec2-transitgateway` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un gateway di transito Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gateway di transito non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gateway di transito non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gateway di transito EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/5.3, benchmark AWS CIS Foundations v3.0. 0/5.2, PCI DSS versione 4.0. 1/1.3.1, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-01.05, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Configurazione di rete sicura > Configurazione del gruppo di sicurezza

Gravità: alta

Tipo di risorsa: `AWS::EC2::SecurityGroup`

Regola AWS Config : `vpc-sg-port-restriction-check`

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`ipType`	La versione IP	Stringa	Non personalizzabile	`IPv4`
`restrictPorts`	Elenco di porte che dovrebbero rifiutare il traffico in ingresso	IntegerList	Non personalizzabile	`22,3389`

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 consente l'ingresso da 0.0.0. 0/0 alle porte di amministrazione remota del server (porte 22 e 3389). Il controllo fallisce se il gruppo di sicurezza consente l'ingresso da 0.0.0. 0/0 alla porta 22 o 3389.

I gruppi di sicurezza forniscono filtraggio stateful del traffico di rete in entrata e in uscita a risorse AWS . È consigliabile che nessun gruppo di sicurezza consenta l'accesso illimitato in ingresso alle porte di amministrazione remota del server, come SSH alla porta 22 e RDP alla porta 3389, utilizzando i protocolli TDP (6), UDP (17) o ALL (-1). Consentire l'accesso pubblico a queste porte aumenta la superficie di attacco delle risorse e il rischio di compromissione delle risorse.

Correzione

Per aggiornare una regola del gruppo di sicurezza EC2 per vietare il traffico in ingresso verso le porte specificate, consulta Update security group rules nella Amazon EC2 User Guide. Dopo aver selezionato un gruppo di sicurezza nella console Amazon EC2, scegli Azioni, Modifica regole in entrata. Rimuovi la regola che consente l'accesso alla porta 22 o alla porta 3389.

[EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/5.4, benchmark AWS CIS Foundations v3.0. 0/5.3, PCI DSS versione 4.0. 1/1.3.1, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-01.05, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Configurazione di rete sicura > Configurazione del gruppo di sicurezza

Gravità: alta

Tipo di risorsa: `AWS::EC2::SecurityGroup`

Regola AWS Config : `vpc-sg-port-restriction-check`

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`ipType`	La versione IP	Stringa	Non personalizzabile	`IPv6`
`restrictPorts`	Elenco di porte che dovrebbero rifiutare il traffico in ingresso	IntegerList	Non personalizzabile	`22,3389`

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 consente l'accesso da: :/0 alle porte di amministrazione del server remoto (porte 22 e 3389). Il controllo fallisce se il gruppo di sicurezza consente l'ingresso da: :/0 alla porta 22 o 3389.

I gruppi di sicurezza forniscono filtraggio stateful del traffico di rete in entrata e in uscita a risorse AWS . È consigliabile che nessun gruppo di sicurezza consenta l'accesso illimitato in ingresso alle porte di amministrazione remota del server, come SSH alla porta 22 e RDP alla porta 3389, utilizzando i protocolli TDP (6), UDP (17) o ALL (-1). Consentire l'accesso pubblico a queste porte aumenta la superficie di attacco delle risorse e il rischio di compromissione delle risorse.

Correzione

Per aggiornare una regola del gruppo di sicurezza EC2 per vietare il traffico in ingresso verso le porte specificate, consulta Update security group rules nella Amazon EC2 User Guide. Dopo aver selezionato un gruppo di sicurezza nella console Amazon EC2, scegli Azioni, Modifica regole in entrata. Rimuovi la regola che consente l'accesso alla porta 22 o alla porta 3389.

[EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR

Requisiti correlati: 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), (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

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Gravità: media

Tipo di risorsa:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Regola AWS Config : vpc-endpoint-enabled

Tipo di pianificazione: periodica

Parametri:

Parametro	Obbligatorio	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`serviceNames`	Richiesto	Il nome del servizio valutato dal controllo	Stringa	Non personalizzabile	`ecr.api`
`vpcIds`	Facoltativo	Comma-separated elenco di ID Amazon VPC per endpoint VPC. Se fornito, il controllo fallisce se i servizi specificati nel	StringList	Personalizza con uno o più ID VPC	Nessun valore predefinito

Parametro	Obbligatorio	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
		`serviceName` parametro non dispongono di uno di questi endpoint VPC.			

Questo controllo verifica se un cloud privato virtuale (VPC) che gestisci dispone di un endpoint VPC di interfaccia per l'API Amazon ECR. Il controllo fallisce se il VPC non dispone di un endpoint VPC di interfaccia per l'API ECR. Questo controllo valuta le risorse in un singolo account.

AWS PrivateLink consente ai clienti di accedere ai servizi ospitati AWS in modo altamente disponibile e scalabile, mantenendo tutto il traffico di rete all'interno della AWS rete. Gli utenti del servizio possono accedere in modo privato ai servizi forniti PrivateLink dal proprio VPC o dall'ambiente locale, senza utilizzare IP pubblici e senza richiedere che il traffico attraversi su Internet.

Correzione

Per configurare un endpoint VPC, consulta Accedere e Servizio AWS utilizzare un endpoint VPC di interfaccia nella Guida.AWS PrivateLink

[EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry

Requisiti correlati: 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), (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

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Gravità: media

Tipo di risorsa:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Regola AWS Config : vpc-endpoint-enabled

Tipo di pianificazione: periodica

Parametri:

Parametro	Obbligatorio	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`serviceNames`	Richiesto	Il nome del servizio valutato dal controllo	Stringa	Non personalizzabile	`ecr.dkr`
`vpcIds`	Facoltativo	Comma-separated elenco di ID Amazon VPC per endpoint VPC. Se fornito, il controllo fallisce se i servizi specificati nel `serviceName` parametro non dispongon	StringList	Personalizza con uno o più ID VPC	Nessun valore predefinito

Parametro	Obbligatorio	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
		o di uno di questi endpoint VPC.			

Questo controllo verifica se un cloud privato virtuale (VPC) che gestisci ha un endpoint VPC di interfaccia per Docker Registry. Il controllo fallisce se il VPC non dispone di un endpoint VPC di interfaccia per Docker Registry. Questo controllo valuta le risorse in un singolo account.

AWS PrivateLink consente ai clienti di accedere ai servizi ospitati AWS in modo altamente disponibile e scalabile, mantenendo tutto il traffico di rete all'interno della AWS rete. Gli utenti del servizio possono accedere in modo privato ai servizi forniti PrivateLink dal proprio VPC o dall'ambiente locale, senza utilizzare IP pubblici e senza richiedere che il traffico attraversi su Internet.

Correzione

Per configurare un endpoint VPC, consulta Accedere e Servizio AWS utilizzare un endpoint VPC di interfaccia nella Guida.AWS PrivateLink

[EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager

Requisiti correlati: 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)

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Gravità: media

Tipo di risorsa:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Regola AWS Config : vpc-endpoint-enabled

Tipo di pianificazione: periodica

Parametri:

Parametro	Obbligatorio	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`serviceNames`	Richiesto	Il nome del servizio valutato dal controllo	Stringa	Non personalizzabile	`ssm`
`vpcIds`	Facoltativo	Comma-separated elenco di ID Amazon VPC per endpoint VPC. Se fornito, il controllo fallisce se i servizi specificati nel `serviceName` parametro non dispongono di uno di questi endpoint VPC.	StringList	Personalizza con uno o più ID VPC	Nessun valore predefinito

Questo controllo verifica se un cloud privato virtuale (VPC) che gestisci dispone di un'interfaccia per un endpoint VPC. AWS Systems Manager Il controllo fallisce se il VPC non dispone di un endpoint VPC di interfaccia per Systems Manager. Questo controllo valuta le risorse in un singolo account.

AWS PrivateLink consente ai clienti di accedere ai servizi ospitati AWS in modo altamente disponibile e scalabile, mantenendo tutto il traffico di rete all'interno della AWS rete. Gli utenti del servizio possono accedere in modo privato ai servizi forniti PrivateLink dal proprio VPC o dall'ambiente locale, senza utilizzare IP pubblici e senza richiedere che il traffico attraversi su Internet.

Correzione

Per configurare un endpoint VPC, consulta Accedere e Servizio AWS utilizzare un endpoint VPC di interfaccia nella Guida.AWS PrivateLink

[EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts

Requisiti correlati: 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)

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Gravità: media

Tipo di risorsa:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Regola AWS Config : vpc-endpoint-enabled

Tipo di pianificazione: periodica

Parametri:

Parametro	Obbligatorio	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`serviceNames`	Richiesto	Il nome del servizio valutato dal controllo	Stringa	Non personalizzabile	`ssm-contacts`
`vpcIds`	Facoltativo	Comma-separated elenco di ID Amazon VPC per endpoint VPC. Se fornito, il controllo fallisce se i servizi specificati nel `serviceName` parametro non dispongono di uno di questi endpoint VPC.	StringList	Personalizza con uno o più ID VPC	Nessun valore predefinito

Questo controllo verifica se un cloud privato virtuale (VPC) che gestisci dispone di un endpoint VPC di interfaccia per Incident Manager Contacts. AWS Systems Manager Il controllo fallisce se il VPC

non dispone di un endpoint VPC di interfaccia per Systems Manager Incident Manager Contacts. Questo controllo valuta le risorse in un singolo account.

AWS PrivateLink consente ai clienti di accedere ai servizi ospitati AWS in modo altamente disponibile e scalabile, mantenendo tutto il traffico di rete all'interno della AWS rete. Gli utenti del servizio possono accedere in modo privato ai servizi forniti PrivateLink dal proprio VPC o dall'ambiente locale, senza utilizzare IP pubblici e senza richiedere che il traffico attraversi su Internet.

Correzione

Per configurare un endpoint VPC, consulta Accedere e Servizio AWS utilizzare un endpoint VPC di interfaccia nella Guida.AWS PrivateLink

[EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager

Requisiti correlati: 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)

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Gravità: media

Tipo di risorsa:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Regola AWS Config : vpc-endpoint-enabled

Tipo di pianificazione: periodica

Parametri:

Parametro	Obbligatorio	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`serviceNames`	Richiesto	Il nome del servizio	Stringa	Non personalizzabile	`ssm-incidents`

Parametro	Obbligatorio	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
		valutato dal controllo			
`vpcIds`	Facoltativo	Comma-separated elenco di ID Amazon VPC per endpoint VPC. Se fornito, il controllo fallisce se i servizi specificati nel `serviceName` parametro non dispongono di uno di questi endpoint VPC.	StringList	Personalizza con uno o più ID VPC	Nessun valore predefinito

Questo controllo verifica se un cloud privato virtuale (VPC) che gestisci ha un'interfaccia VPC endpoint per Incident Manager. AWS Systems Manager Il controllo fallisce se il VPC non dispone di un endpoint VPC di interfaccia per Systems Manager Incident Manager. Questo controllo valuta le risorse in un singolo account.

AWS PrivateLink consente ai clienti di accedere ai servizi ospitati AWS in modo altamente disponibile e scalabile, mantenendo tutto il traffico di rete all'interno della AWS rete. Gli utenti del servizio possono accedere in modo privato ai servizi forniti PrivateLink dal proprio VPC o dall'ambiente locale, senza utilizzare IP pubblici e senza richiedere che il traffico attraversi su Internet.

Correzione

Per configurare un endpoint VPC, consulta Accedere e Servizio AWS utilizzare un endpoint VPC di interfaccia nella Guida.AWS PrivateLink

[EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)

Requisiti correlati: PCI DSS v4.0. 1/22.2.6, Profilo CRI v2. 2/PR. AA-04.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Sicurezza di rete

Gravità: bassa

Tipo di risorsa: `AWS::EC2::LaunchTemplate`

Regola AWS Config : ec2-launch-template-imdsv2-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un modello di lancio di Amazon EC2 è configurato con Instance Metadata Service Version 2 (IMDSv2). Il controllo fallisce se è impostato su. `HttpTokens optional`

L'esecuzione delle risorse sulle versioni software supportate garantisce prestazioni ottimali, sicurezza e accesso alle funzionalità più recenti. Gli aggiornamenti regolari proteggono dalle vulnerabilità, il che aiuta a garantire un'esperienza utente stabile ed efficiente.

Correzione

Per richiedere IMDSv2 su un modello di lancio EC2, consulta Configura le opzioni del servizio di metadati dell'istanza nella Amazon EC2 User Guide.

[EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata

Requisiti correlati: CIS AWS Foundations Benchmark v3.0. 0/5.3, PCI DSS versione 4.0. 1/10.4.2, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::EC2::VPNConnection`

Regola AWS Config : ec2-vpn-connection-logging-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una connessione AWS Site-to-Site VPN ha Amazon CloudWatch Logs abilitato per entrambi i tunnel. Il controllo fallisce se una connessione Site-to-Site VPN non ha CloudWatch i log abilitati per entrambi i tunnel.

AWS Site-to-Site I log VPN ti offrono una visibilità più approfondita sulle tue Site-to-Site implementazioni VPN. Con questa funzionalità, hai accesso ai registri delle connessioni Site-to-Site VPN che forniscono dettagli sulla creazione del tunnel IP Security (IPSec), sulle negoziazioni IKE (Internet Key Exchange) e sui messaggi del protocollo Dead Peer Detection (DPD). Site-to-Site I log VPN possono essere pubblicati in Logs. CloudWatch Questa funzionalità offre ai clienti un unico modo coerente per accedere e analizzare i log dettagliati di tutte le loro Site-to-Site connessioni VPN.

Correzione

Per abilitare la registrazione del tunnel su una connessione VPN EC2, consulta i log AWS Site-to-Site VPN nella Guida per l'utente della AWS Site-to-Site VPN.

[EC2.172] Le impostazioni VPC Block Public Access di EC2 dovrebbero bloccare il traffico del gateway Internet

Categoria: Protezione > Configurazione sicura della rete > Risorse non accessibili al pubblico

Gravità: media

Tipo di risorsa: `AWS::EC2::VPCBlockPublicAccessOptions`

AWS Config regola: `ec2-vpc-bpa-internet-gateway-blocked` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`vpcBpaInternetGatewayBlockMode`	Valore stringa della modalità opzioni VPC BPA.	Enum	`block-bidirectional` , `block-ingress`	Nessun valore predefinito

Questo controllo verifica se le impostazioni di Amazon EC2 VPC Block Public Access (BPA) sono configurate per bloccare il traffico del gateway Internet per tutti i VPC Amazon nel. Account AWS Il controllo fallisce se le impostazioni VPC BPA non sono configurate per bloccare il traffico del gateway Internet. Affinché il controllo passi, il VPC BPA `InternetGatewayBlockMode` deve essere impostato su o. `block-bidirectional` `block-ingress` Se `vpcBpaInternetGatewayBlockMode` viene fornito il parametro, il controllo passa solo se il valore VPC BPA per `InternetGatewayBlockMode` corrisponde al parametro.

La configurazione delle impostazioni VPC BPA per il tuo account in Regione AWS an ti consente di impedire alle risorse in VPC e sottoreti di tua proprietà in quella regione di raggiungere o essere raggiunte da Internet tramite gateway Internet e gateway Internet solo in uscita. Se hai bisogno di VPC e sottoreti specifici per poter raggiungere o essere raggiungibile da Internet, puoi escluderli configurando le esclusioni VPC BPA. Per istruzioni su come creare ed eliminare esclusioni, consulta Creare ed eliminare esclusioni nella Amazon VPC User Guide.

Correzione

Per abilitare il BPA bidirezionale a livello di account, consulta Abilita la modalità bidirezionale BPA per il tuo account nella Amazon VPC User Guide. Per abilitare il BPA solo in ingresso, consulta Modificare la modalità VPC BPA in solo ingresso. Per abilitare VPC BPA a livello di organizzazione, consulta Abilitare VPC BPA a livello di organizzazione.

[EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati

Requisiti correlati: CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::EC2::SpotFleet`

Regola AWS Config : ec2-spot-fleet-request-ct-encryption-at-rest

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una richiesta Amazon EC2 Spot Fleet che specifica i parametri di avvio è configurata per abilitare la crittografia per tutti i volumi Amazon Elastic Block Store (Amazon EBS) collegati alle istanze EC2. Il controllo fallisce se la richiesta Spot Fleet specifica i parametri di avvio e non abilita la crittografia per uno o più volumi EBS specificati nella richiesta.

Per un ulteriore livello di sicurezza, è necessario abilitare la crittografia per i volumi Amazon EBS. Le operazioni di crittografia vengono quindi eseguite sui server che ospitano le istanze Amazon EC2, il che aiuta a garantire la sicurezza sia dei dati inattivi che dei dati in transito tra un'istanza e lo storage EBS collegato. La crittografia Amazon EBS è una soluzione di crittografia semplice per le risorse EBS associate alle tue istanze EC2. Con la crittografia EBS, non è necessario creare, mantenere e proteggere la propria infrastruttura di gestione delle chiavi. La crittografia EBS viene utilizzata AWS KMS keys durante la creazione di volumi crittografati.

> **Note**
>
> Questo controllo non genera risultati per le richieste di Amazon EC2 Spot Fleet che utilizzano modelli di lancio. Inoltre, non genera risultati per le richieste Spot Fleet che non specificano esplicitamente un valore per il `encrypted` parametro.

Correzione

Non esiste un modo diretto per crittografare un volume Amazon EBS esistente e non crittografato. Puoi crittografare un nuovo volume solo quando lo crei.

Tuttavia, se abiliti la crittografia per impostazione predefinita, Amazon EBS crittografa i nuovi volumi utilizzando la tua chiave predefinita per la crittografia EBS. Se non abiliti la crittografia per impostazione predefinita, puoi abilitarla quando crei un singolo volume. In entrambi i casi, puoi sostituire la chiave predefinita per la crittografia EBS e scegliere una chiave gestita dal cliente. AWS KMS key Per ulteriori informazioni sulla crittografia EBS, consulta Amazon EBS encryption nella Amazon EBS User Guide.

Per informazioni sulla creazione di una richiesta Amazon EC2 Spot Fleet, consulta Create a Spot Fleet nella Amazon Elastic Compute Cloud User Guide.

[EC2.174] I set di opzioni DHCP EC2 devono essere etichettati

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::DHCPOptions`

Regola AWS Config : ec2-dhcp-options-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un set di opzioni DHCP di Amazon EC2 ha le chiavi dei tag specificate dal parametro. `requiredKeyTags` Il controllo fallisce se il set di opzioni non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'insieme di opzioni non contiene chiavi di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare,

organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un set di opzioni DHCP di Amazon EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.175] I modelli di lancio di EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::LaunchTemplate`

Regola AWS Config : ec2-launch-template-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfan	Nessun valore predefinito

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	valutata. I tag fanno distinzione tra maiuscole e minuscole		o i requisiti AWS .	

Questo controllo verifica se un modello di lancio di Amazon EC2 ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo fallisce se il modello di lancio non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il modello di avvio non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un modello di lancio di Amazon EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::PrefixList`

Regola AWS Config : ec2-prefix-list-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un elenco di prefissi Amazon EC2 contiene le chiavi dei tag specificate dal parametro. `requiredKeyTags` Il controllo ha esito negativo se l'elenco dei prefissi non contiene alcuna chiave di tag o non contiene tutte le chiavi specificate dal parametro. `requiredKeyTags` Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'elenco dei prefissi non contiene chiavi di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle

strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un elenco di prefissi Amazon EC2, consulta Tagga le risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::TrafficMirrorSession`

Regola AWS Config : ec2-traffic-mirror-session-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfan	Nessun valore predefinito

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	valutata. I tag fanno distinzione tra maiuscole e minuscole		o i requisiti AWS .	

Questo controllo verifica se una sessione di Traffic Mirror di Amazon EC2 ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo fallisce se la sessione non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la sessione non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a una sessione di Traffic Mirror di Amazon EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::TrafficMirrorFilter`

Regola AWS Config : ec2-traffic-mirror-filter-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un filtro Traffic Mirror di Amazon EC2 ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo fallisce se il filtro non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il filtro non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle

strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un filtro Traffic Mirror di Amazon EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::TrafficMirrorTarget`

Regola AWS Config : ec2-traffic-mirror-target-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un target del Traffic Mirror di Amazon EC2 ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo fallisce se la destinazione non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la destinazione non dispone di chiavi di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un target di traffico mirror di Amazon EC2, consulta Tagga le tue risorse Amazon EC2 nella Amazon EC2 User Guide.

[EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination

Requisiti correlati: CRI Profile v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Sicurezza di rete

Gravità: media

Tipo di risorsa: `AWS::EC2::NetworkInterface`

Regola AWS Config : ec2-enis-source-destination-check-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il source/destination controllo è abilitato per un'interfaccia di rete elastica (ENI) di Amazon EC2 gestita dagli utenti. Il controllo fallisce se il source/destination controllo è disabilitato per l'ENI gestito dall'utente. Questo controllo verifica solo i seguenti tipi di ENI:`aws_codestar_connections_managed`,,`branch`, `efa` `interfacelambda`, e. `quicksight`

Source/destination il controllo delle istanze Amazon EC2 e degli ENI collegati deve essere abilitato e configurato in modo coerente su tutte le istanze EC2. Ogni ENI ha le proprie impostazioni per i controlli. source/destination Se il source/destination controllo è abilitato, Amazon EC2 applica la convalida degli source/destination indirizzi, che garantisce che un'istanza sia l'origine o la destinazione di tutto il traffico che riceve. Ciò fornisce un ulteriore livello di sicurezza della rete impedendo alle risorse di gestire traffico involontario e prevenendo lo spoofing degli indirizzi IP.

> **Note**
>
> Se utilizzi un'istanza EC2 come istanza NAT e hai disabilitato il source/destination controllo dell'ENI, puoi invece utilizzare un gateway NAT.

Correzione

Per informazioni sull'abilitazione source/destination dei controlli per un Amazon EC2 ENI, consulta Modificare gli attributi dell'interfaccia di rete nella Amazon EC2 User Guide.

[EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati

Requisiti correlati: CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::EC2::LaunchTemplate`

Regola AWS Config : ec2-launch-templates-ebs-volume-encrypted

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un modello di lancio di Amazon EC2 abilita la crittografia per tutti i volumi EBS collegati. Il controllo fallisce se il parametro di crittografia è impostato su qualsiasi volume EBS specificato dal modello di lancio EC2. `False`

La crittografia Amazon EBS è una soluzione di crittografia semplice per le risorse EBS associate alle istanze Amazon EC2. Con la crittografia EBS, non è necessario creare, mantenere e proteggere la propria infrastruttura di gestione delle chiavi. La crittografia EBS AWS KMS keys viene utilizzata durante la creazione di volumi e istantanee crittografati. Le operazioni di crittografia avvengono sui server che ospitano le istanze EC2, il che aiuta a garantire la sicurezza dei dati inattivi e dei dati in transito tra un'istanza EC2 e lo storage EBS collegato. Per ulteriori informazioni, consulta Crittografia Amazon EBS nella Guida per l'utente di Amazon EBS.

Puoi abilitare la crittografia EBS durante gli avvii manuali di singole istanze EC2. Tuttavia, ci sono diversi vantaggi nell'utilizzare i modelli di avvio EC2 e nella configurazione delle impostazioni di crittografia in tali modelli. È possibile applicare la crittografia come standard e garantire l'uso di impostazioni di crittografia coerenti. È inoltre possibile ridurre il rischio di errori e lacune di sicurezza che potrebbero verificarsi con l'avvio manuale delle istanze.

> **Note**
>
> Quando questo controllo verifica un modello di avvio EC2, valuta solo le impostazioni di crittografia EBS specificate esplicitamente dal modello. La valutazione non include le impostazioni di crittografia ereditate dalle impostazioni di crittografia EBS a livello di account, dalle mappature dei dispositivi a blocchi AMI o dagli stati di crittografia degli snapshot di origine.

Correzione

Dopo aver creato un modello di lancio di Amazon EC2, non puoi modificarlo. Tuttavia, puoi creare una nuova versione di un modello di lancio e modificare le impostazioni di crittografia in quella nuova versione del modello. Puoi anche specificare la nuova versione come versione predefinita del modello di lancio. Quindi, se avvii un'istanza EC2 da un modello di avvio e non specifichi una versione del modello, EC2 utilizza le impostazioni della versione predefinita quando avvia l'istanza. Per ulteriori informazioni, consulta Modificare un modello di lancio nella Amazon EC2 User Guide.

[EC2.182] Le impostazioni di blocco dell'accesso pubblico devono essere abilitate per gli snapshot di Amazon EBS

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::EC2::SnapshotBlockPublicAccess`

Regola AWS Config : ebs-snapshot-block-public-access

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il blocco dell'accesso pubblico a livello di account è abilitato per impedire la condivisione degli snapshot di Amazon EBS con tutti. Il controllo fallisce se il blocco dell'accesso pubblico non è abilitato per bloccare la condivisione degli snapshot di Amazon EBS con tutti.

Per impedire la condivisione pubblica degli snapshot di Amazon EBS, puoi abilitare l'accesso pubblico a blocchi per gli snapshot. Una volta abilitato l'accesso pubblico a blocchi per le istantanee in una regione, qualsiasi tentativo di condividere pubblicamente le istantanee in quella regione viene automaticamente bloccato. Questo aiuta a migliorare la sicurezza delle istantanee e a proteggere i dati delle istantanee da accessi non autorizzati o non intenzionali.

Correzione

Per abilitare l'accesso pubblico a blocchi per gli snapshot, consulta Configurare l'accesso pubblico a blocchi per gli snapshot di Amazon EBS nella Amazon EBS User Guide. Per Blocca l'accesso pubblico, scegli Blocca tutti gli accessi pubblici.

[EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::EC2::VPNConnection`

Regola AWS Config : ec2-vpn-connection-ike-version-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una connessione AWS Site-to-Site VPN è configurata per utilizzare il protocollo IKEv2. Il controllo fallisce se una connessione Site-to-Site VPN consente il protocollo IKEv1 o non si limita esplicitamente a IKEv2 su tutti i tunnel VPN.

IKEv2 offre algoritmi crittografici più potenti e funzionalità di sicurezza migliorate rispetto al protocollo IKEv1 precedente, inclusa una protezione integrata contro gli attacchi di tipo denial-of-service e meccanismi di autenticazione avanzati. IKEv1 presenta vulnerabilità e punti deboli noti nel processo di scambio delle chiavi che possono essere sfruttati dagli aggressori per compromettere la sicurezza del tunnel VPN. Rafforzando IKEv2-only le connessioni, riduci la superficie di attacco e garantisci che le comunicazioni VPN utilizzino protocolli di crittografia moderni e standard del settore che proteggono meglio i dati in transito.

Correzione

Per aggiornare la versione IKE per un tunnel VPN su una connessione VPN EC2, consulta Modificare le opzioni del tunnel VPN nella Guida per l'utente AWS Site-to-Site VPN.AWS Site-to-Site

Controlli CSPM di Security Hub per Auto Scaling

Questi controlli CSPM di Security Hub valutano il servizio e le risorse di Amazon EC2 Auto Scaling.

Questi controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[AutoScaling.1] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB

Requisiti correlati: PCI DSS v3.2. 1/2.2,, NIST.800-53.r5 CP-2 (2) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2 Profilo CRI v2. 2/GV. RM-09.02, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Identificazione > Inventario

Gravità: bassa

Tipo di risorsa: `AWS::AutoScaling::AutoScalingGroup`

Regola AWS Config : `autoscaling-group-elb-healthcheck-required`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo Amazon EC2 Auto Scaling associato a un sistema di bilanciamento del carico utilizza i controlli di integrità Elastic Load Balancing (ELB). Il controllo fallisce se il gruppo Auto Scaling non utilizza i controlli di integrità ELB.

I controlli di integrità ELB aiutano a garantire che un gruppo di Auto Scaling possa determinare lo stato di un'istanza sulla base di test aggiuntivi forniti dal sistema di bilanciamento del carico. L'utilizzo dei controlli di integrità di Elastic Load Balancing aiuta anche a supportare la disponibilità delle applicazioni che utilizzano i gruppi di Auto Scaling EC2.

Correzione

Per aggiungere i controlli di integrità di Elastic Load Balancing, consulta Add Elastic Load Balancing health check nella Amazon EC2 Auto Scaling User Guide.

[AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità

Requisiti correlati: 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 Profile v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::AutoScaling::AutoScalingGroup`

Regola AWS Config : `autoscaling-multiple-az`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`minAvailabilityZones`	Numero minimo di zone di disponibilità	Enum	`2, 3, 4, 5, 6`	`2`	

Questo controllo verifica se un gruppo Amazon EC2 Auto Scaling copre almeno il numero specificato di zone di disponibilità (AZ). Il controllo fallisce se un gruppo di Auto Scaling non copre almeno il numero specificato di AZ. A meno che non si fornisca un valore di parametro personalizzato per il numero minimo di AZ, Security Hub CSPM utilizza un valore predefinito di due AZ.

Un gruppo di Auto Scaling che non si estende su più AZ non può avviare istanze in un'altra AZ per compensare se la singola AZ configurata non è più disponibile. Tuttavia, un gruppo di Auto Scaling con una singola zona di disponibilità può essere preferito in alcuni casi d'uso, come i lavori in batch o quando i costi di trasferimento tra le AZ devono essere ridotti al minimo. In questi casi, è possibile disabilitare questo controllo o eliminarne i risultati.

Correzione

Per aggiungere AZ a un gruppo Auto Scaling esistente, consulta Aggiungere e rimuovere zone di disponibilità nella Guida per l'utente di Amazon EC2 Auto Scaling.

[AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)

Requisiti correlati: NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, (7), NIST.800-53.r5 AC-3 (1) NIST.800-53.r5 AC-6, NIST.800-53.r5 CA-9 PCI DSS v4.0. NIST.800-53.r5 CM-2 1/2.2.6, Profilo CRI v2. 2/PR. AA-04.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: `AWS::AutoScaling::LaunchConfiguration`

Regola AWS Config : `autoscaling-launchconfig-requires-imdsv2`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se IMDSv2 è abilitato su tutte le istanze lanciate dai gruppi Amazon EC2 Auto Scaling. Il controllo fallisce se la versione di Instance Metadata Service (IMDS) non è inclusa nella configurazione di avvio o è configurata come `token optional`, un'impostazione che consente IMDSv1 o IMDSv2.

IMDS fornisce dati sull'istanza che è possibile utilizzare per configurare o gestire l'istanza in esecuzione.

La versione 2 dell'IMDS aggiunge nuove protezioni che non erano disponibili in IMDSv1 per proteggere ulteriormente le istanze EC2.

Correzione

Un gruppo Auto Scaling è associato a una configurazione di avvio alla volta. Non è possibile modificare una configurazione di avvio dopo averla creata. Per modificare la configurazione di avvio per un gruppo Auto Scaling, usa una configurazione di avvio esistente come base per una nuova configurazione di avvio con iMDSv2 abilitato. Per ulteriori informazioni, consulta Configurare le opzioni dei metadati delle istanze per le nuove istanze nella Guida per l'utente di Amazon EC2.

[AutoScaling.4] La configurazione di avvio del gruppo Auto Scaling non deve avere un limite di hop di risposta ai metadati superiore a 1

> **Important**
>
> Security Hub CSPM ha ritirato questo controllo nell'aprile 2024. Per ulteriori informazioni, consulta Registro delle modifiche per i controlli CSPM di Security Hub.

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: `AWS::AutoScaling::LaunchConfiguration`

Regola AWS Config : `autoscaling-launch-config-hop-limit`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica il numero di hop di rete che un token di metadati può percorrere. Il controllo ha esito negativo se il limite dell'hop di risposta ai metadati è maggiore di. 1

L'Instance Metadata Service (IMDS) fornisce informazioni sui metadati su un'istanza Amazon EC2 ed è utile per la configurazione delle applicazioni. La limitazione della PUT risposta HTTP per il servizio di metadati alla sola istanza EC2 protegge l'IMDS dall'uso non autorizzato.

Il campo Time To Live (TTL) nel pacchetto IP viene ridotto di uno per ogni hop. Questa riduzione può essere utilizzata per garantire che il pacchetto non viaggi al di fuori di EC2. IMDSv2 protegge le istanze EC2 che potrebbero essere state configurate erroneamente come router aperti, firewall di livello 3, VPN, tunnel o dispositivi NAT, impedendo così agli utenti non autorizzati di recuperare i metadati. Con IMDSv2, la PUT risposta che contiene il token segreto non può uscire dall'istanza perché il limite di hop di risposta ai metadati predefinito è impostato su. 1 Tuttavia, se questo valore è maggiore di1, il token può lasciare l'istanza EC2.

Correzione

Per modificare il limite dell'hop di risposta ai metadati per una configurazione di avvio esistente, consulta Modificare le opzioni dei metadati dell'istanza per le istanze esistenti nella Amazon EC2 User Guide.

[Autoscaling.5] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici

Requisiti correlati: 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), PCI DSS v4.0. 1/1.4.4, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::AutoScaling::LaunchConfiguration`

Regola AWS Config : `autoscaling-launch-config-public-ip-disabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la configurazione di avvio associata a un gruppo di Auto Scaling assegna un indirizzo IP pubblico alle istanze del gruppo. Il controllo fallisce se la configurazione di avvio associata assegna un indirizzo IP pubblico.

Le istanze Amazon EC2 in una configurazione di avvio del gruppo Auto Scaling non devono avere un indirizzo IP pubblico associato, tranne in casi limite limitati. Le istanze Amazon EC2

dovrebbero essere accessibili solo da un sistema di bilanciamento del carico anziché essere esposte direttamente a Internet.

Correzione

Un gruppo Auto Scaling è associato a una configurazione di avvio alla volta. Non è possibile modificare una configurazione di avvio dopo averla creata. Per modificare la configurazione di avvio per un gruppo con scalabilità automatica, utilizza una configurazione di avvio esistente come base per una nuova configurazione. Quindi, aggiorna il gruppo Auto Scaling affinché utilizzi la nuova configurazione di avvio. Per istruzioni dettagliate, consulta Modifica della configurazione di avvio per un gruppo Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling. Quando crei la nuova configurazione di avvio, in Configurazione aggiuntiva, per dettagli avanzati, tipo di indirizzo IP, scegli Non assegnare un indirizzo IP pubblico a nessuna istanza.

Dopo aver modificato la configurazione di avvio, Auto Scaling avvia nuove istanze con le nuove opzioni di configurazione. Le istanze esistenti non sono interessate. Per aggiornare un'istanza esistente, ti consigliamo di aggiornare l'istanza o di consentire il ridimensionamento automatico per sostituire gradualmente le istanze più vecchie con quelle più recenti in base alle tue politiche di terminazione. Per ulteriori informazioni sull'aggiornamento delle istanze di Auto Scaling, consulta Update Auto Scaling istances nella Amazon EC2 Auto Scaling User Guide.

[AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità

Requisiti correlati: 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, Profilo CRI v2. 2/GV. RM-09.02, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::AutoScaling::AutoScalingGroup`

Regola AWS Config : `autoscaling-multiple-instance-types`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo Amazon EC2 Auto Scaling utilizza più tipi di istanze. Il controllo fallisce se il gruppo Auto Scaling ha un solo tipo di istanza definito.

È possibile aumentare la disponibilità distribuendo l'applicazione su più tipi di istanze in esecuzione in più zone di disponibilità. Security Hub CSPM consiglia di utilizzare più tipi di istanze in modo che il gruppo Auto Scaling possa avviare un altro tipo di istanza se la capacità delle istanze nelle zone di disponibilità scelte è insufficiente.

Correzione

Per creare un gruppo Auto Scaling con più tipi di istanze, consulta Gruppi di Auto Scaling con più tipi di istanze e opzioni di acquisto nella Guida per l'utente di Amazon EC2 Auto Scaling.

[AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-2, CRI Profile v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Identificazione > Configurazione delle risorse

Gravità: media

Tipo di risorsa: `AWS::AutoScaling::AutoScalingGroup`

Regola AWS Config : `autoscaling-launch-template`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo Amazon EC2 Auto Scaling viene creato da un modello di lancio EC2. Questo controllo fallisce se un gruppo Amazon EC2 Auto Scaling non viene creato con un modello di avvio o se un modello di avvio non è specificato in una politica di istanze miste.

Un gruppo Auto Scaling EC2 può essere creato da un modello di lancio EC2 o da una configurazione di avvio. Tuttavia, l'utilizzo di un modello di avvio per creare un gruppo Auto Scaling garantisce l'accesso alle funzionalità e ai miglioramenti più recenti.

Correzione

Per creare un gruppo Auto Scaling con un modello di lancio EC2, consulta Creare un gruppo Auto Scaling utilizzando un modello di avvio nella Amazon EC2 Auto Scaling User Guide. Per informazioni su come sostituire una configurazione di avvio con un modello di avvio, consulta Replace a launch configuration with a launch template nella Amazon EC2 User Guide.

[AutoScaling.10] I gruppi EC2 Auto Scaling devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::AutoScaling::AutoScalingGroup`

AWS Config regola: `tagged-autoscaling-autoscalinggroup` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un gruppo Amazon EC2 Auto Scaling dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gruppo Auto Scaling non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo Auto Scaling non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli

accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gruppo di Auto Scaling, consulta Gruppi e istanze di Tag Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.

Controlli CSPM del Security Hub per Amazon ECR

Questi controlli CSPM di Security Hub valutano il servizio e le risorse Amazon Elastic Container Registry (Amazon ECR).

Questi controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata

Requisiti correlati: PCI NIST.800-53.r5 RA-5 DSS v4.0. 1/6.2.3, PCI DSS versione 4.0. 1/6.2.4, Profilo CRI v2. 2/ID. RA-01.03, Profilo CRI v2. 2/PR. PS-02.01, Profilo CRI v2. 2/PR. PS-02.02

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: alta

Tipo di risorsa: `AWS::ECR::Repository`

Regola AWS Config : ecr-private-image-scanning-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se in un repository Amazon ECR privato è configurata la scansione delle immagini. Il controllo fallisce se l'archivio ECR privato non è configurato per la scansione in modalità push o la scansione continua.

La scansione delle immagini ECR aiuta a identificare le vulnerabilità del software nelle immagini dei contenitori. La configurazione della scansione delle immagini negli archivi ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

Correzione

Per configurare la scansione delle immagini per un repository ECR, consulta Scansione delle immagini nella Amazon Elastic Container Registry User Guide.

[ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-8 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/DE. CM-09.03, Profilo CRI v2. 2/ID. AM-02.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: media

Tipo di risorsa: `AWS::ECR::Repository`

Regola AWS Config : ecr-private-tag-immutability-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un repository ECR privato ha l'immutabilità dei tag abilitata. Questo controllo ha esito negativo se in un repository ECR privato l'immutabilità dei tag è disabilitata. Questa regola è valida se l'immutabilità dei tag è abilitata e ha il valore. `IMMUTABLE`

Amazon ECR Tag Immutability consente ai clienti di fare affidamento sui tag descrittivi di un'immagine come meccanismo affidabile per tracciare e identificare in modo univoco le immagini. Un tag immutabile è statico, il che significa che ogni tag fa riferimento a un'immagine unica. Ciò migliora l'affidabilità e la scalabilità poiché l'uso di un tag statico porterà sempre alla distribuzione della stessa immagine. Una volta configurata, l'immutabilità dei tag impedisce che i tag vengano sovrascritti, riducendo la superficie di attacco.

Correzione

Per creare un repository con tag immutabili configurati o per aggiornare le impostazioni di mutabilità dei tag di immagine per un repository esistente, consulta Image tag mutability nella Amazon Elastic Container Registry User Guide.

[ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata

Requisiti correlati: 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-08.01, Profilo CRI v2. 2/PR. IR-04.02, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Identificazione > Configurazione delle risorse

Gravità: media

Tipo di risorsa: `AWS::ECR::Repository`

Regola AWS Config : ecr-private-lifecycle-policy-configured

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un repository Amazon ECR ha almeno una policy del ciclo di vita configurata. Questo controllo fallisce se un repository ECR non ha alcuna politica del ciclo di vita configurata.

Le policy del ciclo di vita di Amazon ECR consentono di specificare la gestione del ciclo di vita delle immagini in un repository. Configurando le politiche del ciclo di vita, è possibile automatizzare la pulizia delle immagini non utilizzate e la scadenza delle immagini in base all'età o al numero di immagini. L'automazione di queste attività può aiutarti a evitare l'uso involontario di immagini obsolete nel tuo repository.

Correzione

Per configurare una policy del ciclo di vita, consulta Creating a lifecycle policy preview nella Amazon Elastic Container Registry User Guide.

[ECR.4] Gli archivi pubblici ECR devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::ECR::PublicRepository`

AWS Config regola: `tagged-ecr-publicrepository` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un repository pubblico Amazon ECR dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'archivio pubblico non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'archivio pubblico non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un repository pubblico ECR, consulta Tagging an Amazon ECR public repository nella Amazon Elastic Container Registry User Guide.

[ECR.5] I repository ECR devono essere crittografati e gestiti dal cliente AWS KMS keys

Requisiti correlati: 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

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::ECR::Repository`

Regola AWS Config : ecr-repository-cmk-encryption-enabled

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`kmsKeyArns`	Un elenco di Amazon Resource Names (ARN) AWS KMS keys da includere nella valutazione. Il controllo genera	StringList (massimo 10 articoli)	1—10 ARN di chiavi KMS esistenti. Ad esempio,	Nessun valore predefinito

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	un `FAILED` risultato se un repository ECR non è crittografato con una chiave KMS nell'elenco.		`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`	

Questo controllo verifica se un repository Amazon ECR è crittografato quando è inattivo e gestito da un cliente. AWS KMS key Il controllo fallisce se l'archivio ECR non è crittografato con una chiave KMS gestita dal cliente. Facoltativamente, puoi specificare un elenco di chiavi KMS da includere nel controllo nella valutazione.

Per impostazione predefinita, Amazon ECR crittografa i dati del repository con chiavi gestite di Amazon S3 (SSE-S3), utilizzando un algoritmo. AES-256 Per un controllo aggiuntivo, puoi configurare Amazon ECR per crittografare i dati con un AWS KMS key (SSE-KMS o DSSE-KMS). La chiave KMS può essere: una Chiave gestita da AWS che Amazon ECR crea e gestisce per te e ha l'alias`aws/ecr`, oppure una chiave gestita dal cliente che crei e gestisci nel tuo. Account AWS Con una chiave KMS gestita dal cliente, hai il pieno controllo della chiave. Ciò include la definizione e il mantenimento della politica chiave, la gestione delle sovvenzioni, la rotazione del materiale crittografico, l'assegnazione di tag, la creazione di alias e l'attivazione e la disabilitazione della chiave.

> **Note**
>
> AWS KMS supporta l'accesso multiaccount alle chiavi KMS. Se un archivio ECR è crittografato con una chiave KMS di proprietà di un altro account, questo controllo non esegue controlli tra account quando valuta l'archivio. Il controllo non valuta se Amazon ECR può accedere e utilizzare la chiave durante l'esecuzione di operazioni crittografiche per il repository.

Correzione

Non è possibile modificare le impostazioni di crittografia per un repository ECR esistente. Tuttavia, è possibile specificare diverse impostazioni di crittografia per gli archivi ECR che verranno creati successivamente. Amazon ECR supporta l'uso di diverse impostazioni di crittografia per singoli repository.

Per ulteriori informazioni sulle opzioni di crittografia per i repository ECR, consulta Encryption at rest nella Amazon ECR User Guide. Per ulteriori informazioni sulla gestione dei clienti AWS KMS keys, consulta la Developer AWS KMS keysGuide.AWS Key Management Service

Controlli CSPM del Security Hub per Amazon ECS

Questi controlli CSPM di Security Hub valutano il servizio e le risorse Amazon Elastic Container Service (Amazon ECS). I controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[ECS.2] Ai servizi ECS non dovrebbero essere assegnati automaticamente indirizzi IP pubblici

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::ECS::Service`

AWS Config regola: `ecs-service-assign-public-ip-disabled` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i servizi Amazon ECS sono configurati per assegnare automaticamente indirizzi IP pubblici. Se `AssignPublicIP` lo è, questo controllo fallisce. `ENABLED` Questo controllo viene eseguito se lo `AssignPublicIP` è`DISABLED`.

Un indirizzo IP pubblico è un indirizzo IP raggiungibile da Internet. Se avvii le istanze Amazon ECS con un indirizzo IP pubblico, le istanze Amazon ECS sono raggiungibili da Internet. I servizi Amazon ECS non devono essere accessibili al pubblico, in quanto ciò potrebbe consentire l'accesso involontario ai server delle applicazioni container.

Correzione

Innanzitutto, è necessario creare una definizione di attività per il cluster che utilizzi la modalità di **`awsvpc`** rete e specifichi FARGATE per. `requiresCompatibilities` Quindi, per la configurazione di Compute, scegli Launch type e FARGATE. Infine, per il campo Rete, disattivate l'IP pubblico per disabilitare l'assegnazione automatica degli IP pubblici per il vostro servizio.

[ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/DE. CM-09.03, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.02, Profilo CRI v2. 2/PR. PS-01.03, Profilo CRI v2. 2/PR. PS-01.09

Categoria: Identificazione > Configurazione delle risorse

Gravità: alta

Tipo di risorsa: `AWS::ECS::TaskDefinition`

Regola AWS Config : ecs-task-definition-pid-mode-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le definizioni delle attività di Amazon ECS sono configurate per condividere lo spazio dei nomi dei processi di un host con i relativi contenitori. Il controllo fallisce se la definizione dell'attività condivide lo spazio dei nomi del processo dell'host con i contenitori in esecuzione su di esso. Questo controllo valuta solo l'ultima revisione attiva di una definizione di attività Amazon ECS.

Uno spazio dei nomi PID (Process ID) fornisce la separazione tra i processi. Impedisce la visibilità dei processi di sistema e consente il riutilizzo dei PID, incluso il PID 1. Se lo spazio dei nomi PID dell'host è condiviso con i contenitori, consentirebbe ai contenitori di visualizzare tutti i processi sul sistema host. Ciò riduce i vantaggi dell'isolamento a livello di processo tra l'host e i contenitori. Queste circostanze potrebbero portare all'accesso non autorizzato ai processi sull'host stesso,

inclusa la possibilità di manipolarli e terminarli. I clienti non devono condividere lo spazio dei nomi dei processi dell'host con i contenitori in esecuzione su di esso.

Correzione

Per configurare la `pidMode` definizione di un'attività, consulta i parametri di definizione dell'attività nella Amazon Elastic Container Service Developer Guide.

[ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati

Requisiti correlati: 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

Categoria: Protezione > Gestione sicura degli accessi > Restrizioni all'accesso degli utenti root

Gravità: alta

Tipo di risorsa: `AWS::ECS::TaskDefinition`

Regola AWS Config : ecs-containers-nonprivileged

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il `privileged` parametro nella definizione del contenitore di Amazon ECS Task Definitions è impostato `true` su. Il controllo fallisce se questo parametro è uguale `atrue`. Questo controllo valuta solo l'ultima revisione attiva di una definizione di attività Amazon ECS.

Ti consigliamo di rimuovere i privilegi elevati dalle definizioni delle attività ECS. Quando il parametro privilege è`true`, al contenitore vengono assegnati privilegi elevati sull'istanza del contenitore host (analogamente all'utente root).

Correzione

Per configurare il `privileged` parametro su una definizione di attività, consulta i parametri di definizione avanzata dei container nella Amazon Elastic Container Service Developer Guide.

[ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root

Requisiti correlati: NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 (7),, CRI Profile v2. NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6 2/PR.

DS-01.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.02, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: alta

Tipo di risorsa: `AWS::ECS::TaskDefinition`

Regola AWS Config : ecs-containers-readonly-access

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le definizioni delle attività ECS configurano i contenitori in modo che siano limitati all'accesso in sola lettura ai file system root montati. Il controllo ha esito negativo se il `readonlyRootFilesystem` parametro nelle definizioni dei contenitori della definizione delle attività ECS è impostato su o il parametro non esiste nella definizione del contenitore all'interno della definizione dell'attività. `false` Questo controllo valuta solo l'ultima revisione attiva di una definizione di attività Amazon ECS.

Se il `readonlyRootFilesystem` parametro è impostato su `true` in una definizione di attività Amazon ECS, al contenitore ECS viene concesso l'accesso in sola lettura al relativo file system root. Ciò riduce i vettori di attacco alla sicurezza perché il file system root dell'istanza del contenitore non può essere manomesso o scritto senza supporti espliciti di volume con autorizzazioni di lettura/scrittura per cartelle e directory del file system. L'attivazione di questa opzione rispetta anche il principio del privilegio minimo.

> **Note**
>
> Il `readonlyRootFilesystem` parametro non è supportato per i contenitori Windows. Le definizioni delle attività `runtimePlatform` configurate per specificare una famiglia di `WINDOWS_SERVER` sistemi operativi sono contrassegnate come `NOT_APPLICABLE` e non genereranno risultati per questo controllo.

Correzione

Per consentire a un contenitore Amazon ECS l'accesso in sola lettura al relativo file system root, aggiungi il `readonlyRootFilesystem` parametro alla definizione dell'attività per il contenitore e

imposta il valore del parametro su. `true` Per informazioni sui parametri di definizione delle attività e su come aggiungerli a una definizione di attività, consulta le definizioni delle attività di Amazon ECS e l'aggiornamento di una definizione di attività nella Amazon Elastic Container Service Developer Guide.

[ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/86.2, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.07

Categoria: Protezione > Sviluppo sicuro > Credenziali non codificate

Gravità: alta

Tipo di risorsa: `AWS::ECS::TaskDefinition`

Regola AWS Config : ecs-no-environment-secrets

Tipo di pianificazione: modifica attivata

Parametri**`secretKeys`**:`AWS_ACCESS_KEY_ID`,`AWS_SECRET_ACCESS_KEY`, `ECS_ENGINE_AUTH_DATA` (non personalizzabile)

Questo controllo verifica se il valore chiave di qualsiasi variabile nel `environment` parametro delle definizioni dei contenitori include `AWS_ACCESS_KEY_IDAWS_SECRET_ACCESS_KEY`, o`ECS_ENGINE_AUTH_DATA`. Questo controllo ha esito negativo se una singola variabile di ambiente in qualsiasi definizione di contenitore è uguale a `AWS_ACCESS_KEY_IDAWS_SECRET_ACCESS_KEY`, o. `ECS_ENGINE_AUTH_DATA` Questo controllo non copre le variabili ambientali trasmesse da altre postazioni come Amazon S3. Questo controllo valuta solo l'ultima revisione attiva di una definizione di attività Amazon ECS.

AWS Systems Manager Parameter Store può aiutarti a migliorare il livello di sicurezza della tua organizzazione. Ti consigliamo di utilizzare Parameter Store per archiviare segreti e credenziali anziché passarli direttamente alle istanze del contenitore o inserirli nel codice.

Correzione

Per creare parametri utilizzando SSM, vedere Creazione dei parametri di Systems Manager nella Guida per l'AWS Systems Manager utente. Per ulteriori informazioni sulla creazione di una definizione di attività che specifichi un segreto, consulta Specificare dati sensibili utilizzando Secrets Manager nella Amazon Elastic Container Service Developer Guide.

[ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione

Requisiti correlati: 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), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), CRI Profile v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: alta

Tipo di risorsa: `AWS::ECS::TaskDefinition`

AWS Config regola: ecs-task-definition-log-configuration

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'ultima definizione di attività attiva di Amazon ECS ha una configurazione di registrazione specificata. Il controllo fallisce se la definizione dell'attività non ha la `logConfiguration` proprietà definita o se il valore di `logDriver` è nullo in almeno una definizione di contenitore.

La registrazione aiuta a mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon ECS. La raccolta di dati dalle definizioni delle attività offre visibilità, che può aiutarti a eseguire il debug dei processi e a trovare la causa principale degli errori. Se si utilizza una soluzione di registrazione che non deve essere definita nella definizione dell'attività ECS (ad esempio una soluzione di registrazione di terze parti), è possibile disabilitare questo controllo dopo aver verificato che i log vengano acquisiti e consegnati correttamente.

Correzione

Per definire una configurazione di log per le definizioni delle attività di Amazon ECS, consulta Specificare una configurazione di log nella definizione del task nella Amazon Elastic Container Service Developer Guide.

[ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate

Requisiti correlati: 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. 1/6.3.3, Profilo CRI v2. 2/PR. PS-02.03

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: `AWS::ECS::Service`

Regola AWS Config : ecs-fargate-latest-platform-version

Tipo di pianificazione: modifica attivata

Parametri:

- `latestLinuxVersion: 1.4.0`(non personalizzabile)
- `latestWindowsVersion: 1.0.0`(non personalizzabile)

Questo controllo verifica se i servizi Amazon ECS Fargate eseguono l'ultima versione della piattaforma Fargate. Questo controllo fallisce se la versione della piattaforma non è la più recente.

AWS Fargate le versioni della piattaforma si riferiscono a un ambiente di runtime specifico per l'infrastruttura di attività Fargate, che è una combinazione di versioni di runtime del kernel e del container. Le nuove versioni della piattaforma vengono rilasciate man mano che l'ambiente di runtime si evolve. Ad esempio, può essere rilasciata una nuova versione per aggiornamenti del kernel o del sistema operativo, nuove funzionalità, correzioni di bug o aggiornamenti di sicurezza. Gli aggiornamenti e le patch di sicurezza vengono implementati automaticamente per le attività Fargate. Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma, corregge la versione della AWS piattaforma.

Correzione

Per aggiornare un servizio esistente, inclusa la versione della piattaforma, consulta la sezione Aggiornamento di un servizio nella Amazon Elastic Container Service Developer Guide.

[ECS.12] I cluster ECS devono utilizzare Container Insights

Requisiti correlati: 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

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::ECS::Cluster`

Regola AWS Config : ecs-container-insights-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i cluster ECS utilizzano Container Insights. Questo controllo fallisce se Container Insights non è configurato per un cluster.

Il monitoraggio è una parte importante del mantenimento dell'affidabilità, della disponibilità e delle prestazioni dei cluster Amazon ECS. Usa CloudWatch Container Insights per raccogliere, aggregare e riepilogare metriche e log delle tue applicazioni e microservizi containerizzati. CloudWatch raccoglie automaticamente le metriche per molte risorse, come CPU, memoria, disco e rete. Container Insights fornisce inoltre informazioni diagnostiche, ad esempio errori di riavvio del container, che consentono di isolare i problemi e risolverli in modo rapido. Puoi anche impostare CloudWatch allarmi sulle metriche raccolte da Container Insights.

Correzione

Per utilizzare Container Insights, consulta la sezione Aggiornamento di un servizio nella Amazon CloudWatch User Guide.

[ECS.13] I servizi ECS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::ECS::Service`

AWS Config regola: `tagged-ecs-service` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un servizio Amazon ECS dispone di tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il servizio non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il servizio non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un servizio ECS, consulta Tagging your Amazon ECS resources nella Amazon Elastic Container Service Developer Guide.

[ECS.14] I cluster ECS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::ECS::Cluster`

AWS Config regola: `tagged-ecs-cluster` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un cluster Amazon ECS dispone di tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il cluster non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un cluster ECS, consulta Tagging your Amazon ECS resources nella Amazon Elastic Container Service Developer Guide.

[ECS.15] Le definizioni delle attività ECS devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::ECS::TaskDefinition`

AWS Config regola: `tagged-ecs-taskdefinition` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se una definizione di attività Amazon ECS contiene tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se la definizione dell'attività non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se alla definizione dell'attività non è associata alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una definizione di attività ECS, consulta Tagging your Amazon ECS resources nella Amazon Elastic Container Service Developer Guide.

[ECS.16] I set di attività ECS non devono assegnare automaticamente indirizzi IP pubblici

Requisiti correlati: PCI DSS v4.0. 1/14.4.4, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::ECS::TaskSet`

AWS Config regola: `ecs-taskset-assign-public-ip-disabled` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un set di attività Amazon ECS è configurato per l'assegnazione automatica di indirizzi IP pubblici. Il controllo fallisce se `AssignPublicIP` è impostato su. `ENABLED`

Un indirizzo IP pubblico è raggiungibile da Internet. Se si configura il set di attività con un indirizzo IP pubblico, le risorse associate al set di attività possono essere raggiunte da Internet. I set di attività ECS non dovrebbero essere accessibili al pubblico, in quanto ciò potrebbe consentire l'accesso involontario ai server delle applicazioni container.

Correzione

Per aggiornare un set di attività ECS in modo che non utilizzi un indirizzo IP pubblico, consulta Aggiornare una definizione di attività Amazon ECS utilizzando la console nella Amazon Elastic Container Service Developer Guide.

[ECS.17] Le definizioni delle attività ECS non devono utilizzare la modalità di rete host

Requisiti correlati: 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 Profile v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: `AWS::ECS::TaskDefinition`

Regola AWS Config : ecs-task-definition-network-mode-not-host

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'ultima revisione attiva di una definizione di attività Amazon ECS utilizza la modalità di `host` rete. Il controllo fallisce se l'ultima revisione attiva della definizione del task ECS utilizza la modalità di rete. `host`

Quando si utilizza la modalità di `host` rete, la rete di un contenitore Amazon ECS è collegata direttamente all'host sottostante che esegue il contenitore. Di conseguenza, questa modalità consente ai contenitori di connettersi ai servizi di rete di loopback privati sull'host e di impersonare l'host. Altri svantaggi significativi sono che non è possibile rimappare una porta container quando si utilizza la modalità di `host` rete e non è possibile eseguire più di una singola istanza di un'attività su ciascun host.

Correzione

Per informazioni sulle modalità e le opzioni di rete per le attività di Amazon ECS ospitate su istanze Amazon EC2, consulta le opzioni di task networking di Amazon ECS per il tipo di lancio EC2 nella Amazon Elastic Container Service Developer Guide. Per informazioni sulla creazione di una nuova revisione di una definizione di attività e sulla specificazione di una modalità di rete diversa, consulta Updating an Amazon ECS task definition in quella guida.

Se la definizione di attività di Amazon ECS è stata creata da AWS Batch, consulta Modalità di rete per i AWS Batch lavori per conoscere le modalità di rete e l'utilizzo tipico dei tipi di AWS Batch lavoro e per scegliere un'opzione sicura.

[ECS.18] Le definizioni delle attività ECS devono utilizzare la crittografia in transito per i volumi EFS

Categoria: Proteggi > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ECS::TaskDefinition`

Regola AWS Config : ecs-task-definition-efs-encryption-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'ultima revisione attiva di una definizione di attività Amazon ECS utilizza la crittografia in transito per i volumi EFS. Il controllo fallisce se l'ultima revisione attiva della definizione dell'attività ECS ha la crittografia in transito disabilitata per i volumi EFS.

I volumi Amazon EFS forniscono uno storage di file condiviso semplice, scalabile e persistente da utilizzare con le attività di Amazon ECS. Amazon EFS supporta la crittografia dei dati in transito con Transport Layer Security (TLS). Quando la crittografia dei dati in transito viene dichiarata come opzione di montaggio per il file system EFS, Amazon EFS stabilisce una connessione TLS sicura con il file system EFS al momento del montaggio del file system.

Correzione

Per informazioni sull'attivazione della crittografia in transito per Amazon ECS Task Definition con volumi EFS, consulta la Fase 5: Creare una definizione di attività nella Amazon Elastic Container Service Developer Guide.

[ECS.19] I provider di capacità ECS dovrebbero avere abilitato la protezione gestita dalle terminazioni

Categoria: Proteggi > Protezione dei dati

Gravità: media

Tipo di risorsa: `AWS::ECS::CapacityProvider`

Regola AWS Config : ecs-capacity-provider-termination-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un provider di capacità Amazon ECS ha abilitato la protezione gestita delle terminazioni. Il controllo fallisce se la protezione gestita dalla terminazione non è abilitata su un provider di capacità ECS.

I provider di capacità Amazon ECS gestiscono il dimensionamento dell'infrastruttura per le attività nei cluster. Quando si utilizzano le istanze EC2 per la propria capacità, si utilizza il gruppo Auto Scaling per gestire le istanze EC2. La protezione dalla terminazione gestita consente al dimensionamento automatico del cluster di controllare quali istanze vengono terminate. Quando usi la protezione

da terminazione gestita, Amazon ECS termina solo le istanze EC2 che non dispongono di attività Amazon ECS in esecuzione.

> **Note**
>
> Quando utilizzi la protezione da terminazione gestita, devi utilizzare anche il dimensionamento gestito per farla funzionare.

Correzione

Per abilitare la protezione gestita dalle terminazioni per un provider di capacità Amazon ECS, consulta Updating managed termination protection for Amazon ECS capacity provider nella Amazon Elastic Container Service Developer Guide.

[ECS.20] Le definizioni delle attività ECS devono configurare gli utenti non root nelle definizioni dei container Linux

Categoria: Protezione > Gestione sicura degli accessi > Restrizioni di accesso degli utenti root

Gravità: media

Tipo di risorsa: `AWS::ECS::TaskDefinition`

Regola AWS Config : ecs-task-definition-linux-user-non-root

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'ultima revisione attiva di una definizione di attività di Amazon ECS configura i contenitori Linux per l'esecuzione come utenti non root. Il controllo fallisce se è configurato un utente root predefinito o se la configurazione utente è assente per qualsiasi contenitore.

Quando i contenitori Linux vengono eseguiti con privilegi di root, presentano diversi rischi significativi per la sicurezza. Gli utenti root hanno accesso illimitato all'interno del contenitore. Questo accesso elevato aumenta il rischio di attacchi di fuga dai container, in cui un utente malintenzionato potrebbe potenzialmente uscire dall'isolamento dei container e accedere al sistema host sottostante. Se un container che funziona come root viene compromesso, gli aggressori possono sfruttarlo per accedere o modificare le risorse del sistema host, danneggiando altri contenitori o l'host stesso. Inoltre, l'accesso root potrebbe consentire attacchi di escalation dei privilegi, consentendo agli aggressori di ottenere autorizzazioni aggiuntive oltre all'ambito previsto dal contenitore. Il parametro user nelle

definizioni delle attività ECS può specificare gli utenti in diversi formati, tra cui nome utente, ID utente, nome utente con gruppo o UID con ID di gruppo. È importante essere consapevoli di questi diversi formati durante la configurazione delle definizioni delle attività per garantire che non venga concesso inavvertitamente l'accesso root. Seguendo il principio del privilegio minimo, i contenitori devono funzionare con le autorizzazioni minime richieste utilizzando utenti non root. Questo approccio riduce in modo significativo la potenziale superficie di attacco e mitiga l'impatto di potenziali violazioni della sicurezza.

> **Note**
>
> Questo controllo valuta le definizioni dei contenitori in una definizione di attività solo se `operatingSystemFamily` è configurato come `LINUX` o non `operatingSystemFamily` è configurato nella definizione dell'attività. Il controllo genererà un `FAILED` risultato per una definizione di attività valutata se una definizione di contenitore nella definizione dell'attività `user` non è stata configurata o `user` configurata come utente root predefinito. Gli utenti root predefiniti per i `LINUX` contenitori sono `"root"` e`"0"`.

Correzione

Per informazioni sulla creazione di una nuova revisione di una definizione di attività di Amazon ECS e sull'aggiornamento del `user` parametro nella definizione del contenitore, consulta Updating an Amazon ECS task defintion nella Amazon Elastic Container Service Developer Guide.

[ECS.21] Le definizioni delle attività ECS devono configurare gli utenti non amministratori nelle definizioni dei contenitori Windows

Categoria: Protezione > Gestione sicura degli accessi > Restrizioni di accesso degli utenti root

Gravità: media

Tipo di risorsa: `AWS::ECS::TaskDefinition`

Regola AWS Config : ecs-task-definition-windows-user-non-admin

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'ultima revisione attiva di una definizione di attività di Amazon ECS configura i contenitori Windows per l'esecuzione come utenti che non sono amministratori predefiniti.

Il controllo fallisce se un amministratore predefinito è configurato come utente o la configurazione utente è assente per qualsiasi contenitore.

Quando i contenitori Windows vengono eseguiti con privilegi di amministratore, presentano diversi rischi significativi per la sicurezza. Gli amministratori hanno accesso illimitato all'interno del contenitore. Questo accesso elevato aumenta il rischio di attacchi di fuga dai container, in cui un utente malintenzionato potrebbe potenzialmente uscire dall'isolamento dei container e accedere al sistema host sottostante.

> **Note**
>
> Questo controllo valuta le definizioni dei contenitori in una definizione di attività solo se `operatingSystemFamily` è configurato come `WINDOWS_SERVER` o non `operatingSystemFamily` è configurato nella definizione dell'attività. Il controllo genererà un `FAILED` risultato per una definizione di attività valutata se una definizione di contenitore nella definizione dell'attività `user` non è stata configurata o `user` configurata come amministratore predefinito per `WINDOWS_SERVER` i contenitori, ovvero. `"containeradministrator"`

Correzione

Per informazioni sulla creazione di una nuova revisione di una definizione di attività di Amazon ECS e sull'aggiornamento del `user` parametro nella definizione del contenitore, consulta Updating an Amazon ECS task defintion nella Amazon Elastic Container Service Developer Guide.

Controlli CSPM del Security Hub per Amazon EFS

Questi controlli CSPM di Security Hub valutano il servizio e le risorse Amazon Elastic File System (Amazon EFS). I controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/2.3.1, benchmark AWS CIS Foundations v3.0. 0/2.4.1, 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 (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::EFS::FileSystem`

Regola AWS Config : efs-encrypted-check

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se Amazon Elastic File System è configurato per crittografare i dati dei file utilizzando AWS KMS. Il controllo non riesce nei seguenti casi.

- `Encrypted` è impostato su `false` nella risposta `DescribeFileSystems`.
- La chiave `KmsKeyId` nella risposta `DescribeFileSystems` non corrisponde al parametro `KmsKeyId` per `efs-encrypted-check`.

Questo controllo non utilizza il parametro `KmsKeyId` per `efs-encrypted-check`. Controlla solo il valore di `Encrypted`.

Per un ulteriore livello di sicurezza per i dati sensibili in Amazon EFS, è necessario creare file system crittografati. Amazon EFS supporta la crittografia per i file system inattivi. Puoi abilitare la crittografia dei dati inattivi quando crei un file system Amazon EFS. Per ulteriori informazioni sulla crittografia Amazon EFS, consulta la sezione Crittografia dei dati in Amazon EFS nella Amazon Elastic File System User Guide.

Correzione

Per dettagli su come crittografare un nuovo file system Amazon EFS, consulta Encrypting data at rest nella Amazon Elastic File System User Guide.

[EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup

Requisiti correlati: 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-13 (5) NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-11.01

Categoria: Recupero > Resilienza > Backup

Gravità: media

Tipo di risorsa: `AWS::EFS::FileSystem`

Regola AWS Config : efs-in-backup-plan

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se i file system Amazon Elastic File System (Amazon EFS) vengono aggiunti ai piani di backup in AWS Backup. Il controllo fallisce se i file system Amazon EFS non sono inclusi nei piani di backup.

L'inclusione dei file system EFS nei piani di backup consente di proteggere i dati dall'eliminazione e dalla perdita di dati.

Correzione

Per abilitare i backup automatici per un file system Amazon EFS esistente, consulta Getting started 4: Create backup automatici di Amazon EFS nella AWS Backup Developer Guide.

[EFS.3] I punti di accesso EFS devono applicare una directory principale

Requisiti correlati: NIST.800-53.r5 AC-6 (10), CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. IR-01.05, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.02, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::EFS::AccessPoint`

Regola AWS Config : efs-access-point-enforce-root-directory

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i punti di accesso Amazon EFS sono configurati per applicare una directory principale. Il controllo fallisce se il valore di `Path` è impostato su `/` (la directory principale predefinita del file system).

Quando applichi una directory radice, il client NFS che utilizza il punto di accesso usa la directory radice configurata sul punto di accesso anziché la directory radice del file system. L'applicazione di

una directory principale per un punto di accesso consente di limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano accedere solo ai file della sottodirectory specificata.

Correzione

Per istruzioni su come applicare una directory principale per un punto di accesso Amazon EFS, consulta Implementazione di una directory principale con un punto di accesso nella Amazon Elastic File System User Guide.

[EFS.4] I punti di accesso EFS devono applicare un'identità utente

Requisiti correlati: NIST.800-53.r5 AC-6 (2), PCI DSS v4.0. 1/7.3.1, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. DS-10.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::EFS::AccessPoint`

Regola AWS Config : efs-access-point-enforce-user-identity

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i punti di accesso Amazon EFS sono configurati per applicare un'identità utente. Questo controllo ha esito negativo se non viene definita un'identità utente POSIX durante la creazione del punto di accesso EFS.

I punti di accesso Amazon EFS sono punti di accesso specifici dell'applicazione in un file system EFS che semplificano la gestione dell'accesso dell'applicazione ai set di dati condivisi. I punti di accesso possono applicare un'identità utente, inclusi i gruppi dell'utente POSIX, per tutte le richieste al file system effettuate tramite il punto di accesso. I punti di accesso possono inoltre applicare una directory radice diversa per il file system in modo che i client possano accedere solo ai dati nella directory specificata o nelle sue sottodirectory.

Correzione

Per applicare un'identità utente per un punto di accesso Amazon EFS, consulta Applica un'identità utente utilizzando un punto di accesso nella Amazon Elastic File System User Guide.

[EFS.5] I punti di accesso EFS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EFS::AccessPoint`

AWS Config regola: `tagged-efs-accesspoint` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un punto di accesso Amazon EFS dispone di tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il punto di accesso non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il punto di accesso non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una

singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un punto di accesso EFS, consulta Tagging delle risorse Amazon EFS nella Amazon Elastic File System User Guide.

[EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio

Requisiti correlati: NIST.800-171.r2 3.1.20 NIST.800-53.r5 SC-7, PCI DSS v4.0. 1/1.4.4, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Sicurezza della rete > Risorse non accessibili al pubblico

Gravità: media

Tipo di risorsa: `AWS::EFS::FileSystem`

Regola AWS Config : efs-mount-target-public-accessible

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un target di montaggio Amazon EFS è associato a sottoreti che assegnano indirizzi IP pubblici all'avvio. Il controllo fallisce se la destinazione di montaggio è associata a sottoreti che assegnano indirizzi IP pubblici all'avvio.

Le sottoreti dispongono di attributi che determinano se le interfacce di rete create nella sottorete ricevono automaticamente indirizzi IP pubblici. Per IPv4, l'`MapPublicIpOnLaunch`attributo è

impostato su per le sottoreti predefinite e `TRUE` `FALSE` per le sottoreti non predefinite (ad eccezione delle sottoreti non predefinite create tramite la procedura guidata di avvio dell'istanza EC2, dove è impostato su). `TRUE` Per IPv6, l'attributo è impostato su per tutte le sottoreti per impostazione predefinita. `AssignIpv6AddressOnCreation` `FALSE`

Sebbene agli obiettivi di montaggio di Amazon EFS non sia possibile assegnare indirizzi IPv4 pubblici, collocarli in sottoreti configurate per assegnare indirizzi IP pubblici all'avvio indica che le istanze co-localizzate lanciate in tali sottoreti che possono montare il file system EFS potrebbero ricevere automaticamente indirizzi IP pubblici, il che potrebbe rischiare che i dati del file system diventino accessibili da host con indirizzi pubblici.

Le destinazioni di montaggio in sottoreti con l'assegnazione automatica di indirizzi IPv6 pubblici abilitata possono ricevere indirizzi IPv6 instradabili a livello globale.

> **Note**
>
> Il 3 agosto 2026, Security Hub CSPM ha rimosso questo controllo dallo standard AWS Foundational Security Best Practices (FSBP). Questo controllo sarà disponibile nello standard NIST SP 800-53 Rev. 5, nello standard NIST SP 800-171 Revision 2 e nello standardPCI DSS v4.0.1.

Correzione

Per associare una destinazione di montaggio esistente a una sottorete diversa, è necessario creare una nuova destinazione di montaggio in una sottorete che non assegni indirizzi IP pubblici all'avvio e quindi rimuovere la vecchia destinazione di montaggio. Per informazioni sulla gestione degli obiettivi di montaggio, consulta Creazione e gestione di destinazioni di montaggio e gruppi di sicurezza nella Amazon Elastic File System User Guide.

[EFS.7] I file system EFS devono avere i backup automatici abilitati

Requisiti correlati: CRI Profile v2. 2/PR. DS-11.01

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: `AWS::EFS::FileSystem`

Regola AWS Config : efs-automatic-backups-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un file system Amazon EFS ha i backup automatici abilitati. Questo controllo fallisce se il file system EFS non ha i backup automatici abilitati.

Un backup dei dati è una copia dei dati del sistema, della configurazione o dell'applicazione archiviata separatamente dall'originale. L'attivazione di backup regolari consente di proteggere dati importanti da eventi imprevisti come guasti del sistema, attacchi informatici o eliminazioni accidentali. Una solida strategia di backup facilita anche un ripristino più rapido, la continuità aziendale e la tranquillità di fronte alla potenziale perdita di dati.

Correzione

Per informazioni sull'utilizzo AWS Backup per i file system EFS, consulta Backup up EFS file system nella Amazon Elastic File System User Guide.

[EFS.8] I file system EFS devono essere crittografati quando sono inattivi

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/2.3.1, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06, Profilo CRI v2. 2/PR. PS-01.07

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::EFS::FileSystem`

Regola AWS Config : efs-filesystem-ct-encrypted

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un file system Amazon EFS crittografa i dati con AWS Key Management Service (AWS KMS). Il controllo fallisce se un file system non è crittografato.

I dati inattivi si riferiscono ai dati archiviati in uno storage persistente e non volatile per qualsiasi durata. La crittografia dei dati inutilizzati consente di proteggerne la riservatezza, riducendo il rischio che un utente non autorizzato possa accedervi.

Correzione

Per abilitare la crittografia a riposo per un nuovo file system EFS, consulta Encrypting data at rest nella Amazon Elastic File System User Guide.

Controlli CSPM del Security Hub per Amazon EKS

Questi controlli CSPM di Security Hub valutano il servizio e le risorse Amazon Elastic Kubernetes Service (Amazon EKS). I controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[EKS.1] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico

Requisiti correlati: 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, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.05

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::EKS::Cluster`

Regola AWS Config : eks-endpoint-no-public-access

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un endpoint del cluster Amazon EKS è accessibile pubblicamente. Il controllo fallisce se un cluster EKS ha un endpoint accessibile pubblicamente.

Quando crei un nuovo cluster, Amazon EKS crea un endpoint per il server API Kubernetes gestito che usi per comunicare con il cluster. Per impostazione predefinita, questo endpoint del server API è disponibile pubblicamente su Internet. L'accesso al server API è protetto utilizzando una combinazione di AWS Identity and Access Management (IAM) e RBAC (Role Based Access Control) nativo di Kubernetes. Rimuovendo l'accesso pubblico all'endpoint, puoi evitare l'esposizione e l'accesso involontari al tuo cluster.

Correzione

Per modificare l'accesso agli endpoint per un cluster EKS esistente, consulta Modificare l'accesso agli endpoint del cluster nella Amazon EKS User Guide. Puoi configurare l'accesso agli endpoint per un nuovo cluster EKS al momento della creazione. Per istruzioni sulla creazione di un nuovo cluster Amazon EKS, consulta Creazione di un cluster Amazon EKS nella Guida per l'utente di Amazon EKS.

[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-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. 1/12.3.4, Profilo CRI v2. 2/PR. PS-02.03

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: alta

Tipo di risorsa: `AWS::EKS::Cluster`

Regola AWS Config : eks-cluster-supported-version

Tipo di pianificazione: modifica attivata

Parametri:

- `oldestVersionSupported`: `1.34` (non personalizzabile)

Questo controllo verifica se un cluster Amazon Elastic Kubernetes Service (Amazon EKS) è in esecuzione su una versione Kubernetes con supporto standard. Il controllo fallisce se il cluster Amazon EKS è in esecuzione su una versione di supporto esteso o non supportata.

Se la tua applicazione non richiede una versione specifica di Kubernetes, ti consigliamo di utilizzare l'ultima versione di Kubernetes disponibile supportata da EKS per i tuoi cluster. Per ulteriori informazioni, consulta il calendario delle release di Amazon EKS Kubernetes e Comprendi il ciclo di vita della versione Kubernetes su Amazon EKS nella Guida per l'utente di Amazon EKS.

Correzione

Per aggiornare un cluster EKS, consulta Aggiornare un cluster esistente a una nuova versione di Kubernetes nella Amazon EKS User Guide.

[EKS.6] I cluster EKS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EKS::Cluster`

AWS Config regola: `tagged-eks-cluster` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un cluster Amazon EKS dispone di tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il cluster non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una

singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un cluster EKS, consulta Tagging your Amazon EKS Resources nella Amazon EKS User Guide.

[EKS.7] Le configurazioni dei provider di identità EKS devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EKS::IdentityProviderConfig`

AWS Config regola: `tagged-eks-identityproviderconfig` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfan	Nessun valore predefinito

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	I tag fanno distinzione tra maiuscole e minuscole		o i requisiti AWS .	

Questo controllo verifica se la configurazione di un provider di identità Amazon EKS ha tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se la configurazione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la configurazione non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag alle configurazioni di un provider di identità EKS, consulta Tagging your Amazon EKS resources nella Amazon EKS User Guide.

[EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata

Requisiti correlati: 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), (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 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.2.1, Profilo CRI v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::EKS::Cluster`

Regola AWS Config : eks-cluster-log-enabled

Tipo di pianificazione: modifica attivata

Parametri:

- `logTypes: audit`(non personalizzabile)

Questo controllo verifica se un cluster Amazon EKS ha abilitato la registrazione di audit. Il controllo fallisce se la registrazione di controllo non è abilitata per il cluster.

> **Note**
>
> Questo controllo non verifica se la registrazione di audit di Amazon EKS è abilitata tramite Amazon Security Lake per. Account AWS

La registrazione del piano di controllo EKS fornisce registri di audit e diagnostica direttamente dal piano di controllo EKS ad Amazon CloudWatch Logs nel tuo account. Puoi selezionare i tipi di log di cui hai bisogno e i log vengono inviati come flussi di log a un gruppo per ogni cluster EKS in cui risiede. CloudWatch La registrazione offre visibilità sull'accesso e sulle prestazioni dei cluster EKS. Inviando i log del piano di controllo EKS per i cluster EKS a CloudWatch Logs, è possibile registrare le operazioni a fini di controllo e diagnostica in una posizione centrale.

Correzione

Per abilitare i log di controllo per il tuo cluster EKS, consulta Abilitazione e disabilitazione dei log del piano di controllo nella Guida per l'utente di Amazon EKS.

[EKS.9] I gruppi di nodi EKS devono essere eseguiti su una versione di Kubernetes supportata

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: alta

Tipo di risorsa: `AWS::EKS::Nodegroup`

Regola AWS Config : eks-nodegroup-supported-version-check

Tipo di pianificazione: modifica attivata

Parametri:

- `oldestVersionSupported`: `1.34` (non personalizzabile)

Questo controllo verifica se un gruppo di nodi Amazon EKS funziona su una versione Kubernetes con supporto standard. Il controllo fallisce se il gruppo di nodi Amazon EKS viene eseguito su una versione di supporto estesa o non supportata.

Solo le versioni di Kubernetes con supporto standard ricevono il set completo di patch di sicurezza, correzioni di bug e funzionalità di sicurezza. Le versioni con supporto esteso ricevono patch per vulnerabilità critiche e importanti, ma non ricevono patch per vulnerabilità di gravità inferiore, correzioni di bug non di sicurezza o funzionalità di sicurezza introdotte nelle versioni più recenti di Kubernetes. Amazon EKS non aggiorna automaticamente i gruppi di nodi, quindi le patch a livello di nodo si applicano solo dopo aver aggiornato i gruppi di nodi per utilizzare le più recenti AMI ottimizzate per Amazon EKS. Le versioni che hanno superato la fine del supporto esteso non ricevono più patch di sicurezza, correzioni di bug o aggiornamenti di compatibilità da. AWS Le versioni non supportate possono contenere vulnerabilità note che sono state risolte nelle versioni più recenti e potrebbero presentare problemi di compatibilità con immagini di container aggiornate Servizi AWS e strumenti di terze parti nell'ecosistema Kubernetes. Se la tua applicazione non richiede una versione specifica di Kubernetes, ti consigliamo di utilizzare l'ultima versione di Kubernetes disponibile supportata da Amazon EKS per i tuoi gruppi di nodi. Per ulteriori informazioni, consulta il calendario delle release di Amazon EKS Kubernetes e Understand each phase of node updates nella Amazon EKS User Guide.

Correzione

Per aggiornare un gruppo di nodi EKS, consulta Aggiornare un gruppo di nodi gestiti per il cluster nella Amazon EKS User Guide.

Controlli CSPM Security Hub per ElastiCache

Questi AWS Security Hub CSPM controlli valutano il ElastiCache servizio e le risorse Amazon. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati

Requisiti correlati: 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 SC-5 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13 (5) NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-11.01

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: alta

Tipo di risorsa:, `AWS::ElastiCache::CacheCluster` `AWS:ElastiCache:ReplicationGroup`

Regola AWS Config : elasticache-redis-cluster-automatic-backup-check

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`snapshotRetentionPeriod`	Periodo minimo di conservazione delle istantanee in giorni	Numero intero	Da `1` a `35`	`1`

Questo controllo valuta se un cluster Amazon ElastiCache (Redis OSS) ha i backup automatici abilitati. Il controllo fallisce se il periodo di `SnapshotRetentionLimit` tempo per il cluster Redis OSS è inferiore al periodo di tempo specificato. A meno che non si fornisca un valore di parametro

personalizzato per il periodo di conservazione delle istantanee, Security Hub CSPM utilizza un valore predefinito di 1 giorno.

ElastiCache I cluster (Redis OSS) possono eseguire il backup dei propri dati. Il backup può essere utilizzato per ripristinare un cluster o dare fonte a un nuovo cluster. Il backup è costituito dai metadati del cluster, insieme a tutti i dati del cluster. Tutti i backup vengono scritti su Amazon S3, che fornisce uno storage durevole. Puoi ripristinare i dati creando un nuovo ElastiCache cluster e popolandolo con i dati di un backup. È possibile gestire i backup utilizzando l' Console di gestione AWS AWS CLI, l'e l' ElastiCache API.

> **Note**
>
> Questo controllo valuta anche i gruppi di replica ElastiCache (Redis OSS e Valkey).

Correzione

Per informazioni sulla pianificazione dei backup automatici per un ElastiCache cluster, consulta la sezione Pianificazione dei backup automatici nella Amazon User Guide. ElastiCache

[ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati

Requisiti correlati: 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. 1/6.3.3, Profilo CRI v2. 2/ID. RA-01.03, Profilo CRI v2. 2/PR. PS-02.01

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: alta

Tipo di risorsa: `AWS::ElastiCache::CacheCluster`

Regola AWS Config : elasticache-auto-minor-version-upgrade-check

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo valuta se Amazon applica ElastiCache automaticamente aggiornamenti di versione minori a un cluster di cache. Il controllo fallisce se al cluster di cache non vengono applicati automaticamente aggiornamenti di versione minori.

> **Note**
>
> Questo controllo non si applica ai cluster ElastiCache Memcached.

L'aggiornamento automatico della versione secondaria è una funzionalità che puoi abilitare in Amazon ElastiCache per aggiornare automaticamente i tuoi cluster di cache quando è disponibile una nuova versione del motore di cache secondario. Questi aggiornamenti potrebbero includere patch di sicurezza e correzioni di bug. Rimanere aggiornati sull'installazione delle patch è un passo importante per proteggere i sistemi.

Correzione

Per applicare automaticamente aggiornamenti di versioni minori a un cluster di ElastiCache cache esistente, consulta la sezione Gestione delle versioni ElastiCache nella Amazon ElastiCache User Guide.

[ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-04.02, Profilo CRI v2. 2/RC. RP-01.01

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::ElastiCache::ReplicationGroup`

Regola AWS Config : elasticache-repl-grp-auto-failover-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un gruppo di ElastiCache replica ha il failover automatico abilitato. Il controllo fallisce se il failover automatico non è abilitato per un gruppo di replica.

Quando il failover automatico è abilitato per un gruppo di replica, il ruolo del nodo primario eseguirà automaticamente il failover su una delle repliche di lettura. Questa promozione del failover e della replica consente di riprendere la scrittura sul nuovo sistema primario una volta completata la promozione, riducendo così i tempi di inattività complessivi in caso di guasto.

Correzione

Per abilitare il failover automatico per un gruppo di ElastiCache replica esistente, consulta Modifying an ElastiCache cluster nella Amazon ElastiCache User Guide. Se usi la ElastiCache console, imposta il failover automatico su abilitato.

[ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi

Requisiti correlati: 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, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::ElastiCache::ReplicationGroup`

Regola AWS Config : elasticache-repl-grp-encrypted-at-rest

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un gruppo di ElastiCache replica è crittografato quando è inattivo. Il controllo ha esito negativo se il gruppo di replica non è crittografato a riposo.

La crittografia dei dati inattivi riduce il rischio che un utente non autenticato acceda ai dati archiviati su disco. ElastiCache I gruppi di replica (Redis OSS) devono essere crittografati quando sono inattivi per un ulteriore livello di sicurezza.

Correzione

Per configurare la crittografia a riposo su un gruppo di ElastiCache replica, consulta Enabling at-rest encryption nella Amazon ElastiCache User Guide.

[ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito

Requisiti correlati: 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), PCI DSS v4.0. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ElastiCache::ReplicationGroup`

Regola AWS Config : elasticache-repl-grp-encrypted-in-transit

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un gruppo di ElastiCache replica è crittografato in transito. Il controllo ha esito negativo se il gruppo di replica non è crittografato in transito.

La crittografia dei dati in transito riduce il rischio che un utente non autorizzato possa intercettare il traffico di rete. L'attivazione della crittografia in transito su un gruppo di ElastiCache replica crittografa i dati ogni volta che vengono spostati da un luogo all'altro, ad esempio tra i nodi del cluster o tra il cluster e l'applicazione.

Correzione

Per configurare la crittografia in transito su un gruppo di ElastiCache replica, consulta Enabling in-transit encryption nella Amazon ElastiCache User Guide.

[ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato

Requisiti correlati: 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. 1/8.3.1, Profilo CRI v2. 2/PR. AA-03.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::ElastiCache::ReplicationGroup`

Regola AWS Config : elasticache-repl-grp-redis-auth-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un gruppo di replica ElastiCache (Redis OSS) ha Redis OSS AUTH abilitato. Il controllo ha esito negativo se la versione Redis OSS dei nodi del gruppo di replica è inferiore alla 6.0 e non è in uso. `AuthToken`

Quando si utilizzano token di autenticazione o password Redis, Redis richiede una password prima di consentire ai client di eseguire i comandi, il che migliora la sicurezza dei dati. Per Redis 6.0 e versioni successive, consigliamo di utilizzare Role-Based Access Control (RBAC). Poiché RBAC non è supportato per le versioni di Redis precedenti alla 6.0, questo controllo valuta solo le versioni che non possono utilizzare la funzionalità RBAC.

Correzione

Per utilizzare Redis AUTH su un gruppo di replica ElastiCache (Redis OSS), consulta Modifica del token AUTH su un cluster esistente ElastiCache (Redis OSS) nella Amazon User Guide. ElastiCache

[ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito

Requisiti correlati: 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 Profile v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: `AWS::ElastiCache::CacheCluster`

Regola AWS Config : elasticache-subnet-group-check

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un ElastiCache cluster è configurato con un gruppo di sottoreti personalizzato. Il controllo ha esito negativo se `CacheSubnetGroupName` per un ElastiCache cluster ha il valore`default`.

Quando si avvia un ElastiCache cluster, viene creato un gruppo di sottoreti predefinito se non ne esiste già uno. Il gruppo predefinito utilizza le sottoreti del Virtual Private Cloud (VPC) predefinito. Si consiglia di utilizzare gruppi di sottoreti personalizzati che limitino le sottoreti in cui risiede il cluster e la rete che il cluster eredita dalle sottoreti.

Correzione

Per creare un nuovo gruppo di sottoreti per un ElastiCache cluster, consulta la sezione Creazione di un gruppo di sottoreti nella Amazon ElastiCache User Guide.

Controlli CSPM di Security Hub per Elastic Beanstalk

Questi AWS Security Hub CSPM controlli valutano il AWS Elastic Beanstalk servizio e le risorse.

Questi controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata

Requisiti correlati: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, CRI Profile v2. 2/GV. RM-09.02, Profilo CRI v2. 2/PR. IR-03.01

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: `AWS::ElasticBeanstalk::Environment`

Regola AWS Config : `beanstalk-enhanced-health-reporting-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i report avanzati sullo stato di salute sono abilitati per gli AWS Elastic Beanstalk ambienti in uso.

La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione.

Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare. L'agente sanitario Elastic Beanstalk, incluso nelle AMI (Amazon Machine Images) supportate, valuta i log e i parametri delle istanze EC2 dell'ambiente.

Per ulteriori informazioni, consulta Enhanced Health Reporting and Monitoring nella Developer Guide.AWS Elastic Beanstalk

Correzione

Per istruzioni su come abilitare la reportistica sanitaria avanzata, consulta Enhanced Health Reporting using the Elastic Beanstalk console nella Developer Guide.AWS Elastic Beanstalk

[ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati

Requisiti correlati: 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. 1/6.3.3, Profilo CRI v2. 2/PR. PS-02.01

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: alta

Tipo di risorsa: `AWS::ElasticBeanstalk::Environment`

Regola AWS Config : `elastic-beanstalk-managed-updates-enabled`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`UpdateLevel`	Livello di aggiornamento della versione	Enum	`minor`, `patch`	Nessun valore predefinito

Questo controllo verifica se gli aggiornamenti della piattaforma gestita sono abilitati per un ambiente Elastic Beanstalk. Il controllo fallisce se non sono abilitati gli aggiornamenti gestiti della piattaforma. Per impostazione predefinita, il controllo passa se è abilitato qualsiasi tipo di aggiornamento della piattaforma. Facoltativamente, è possibile fornire un valore di parametro personalizzato per richiedere un livello di aggiornamento specifico.

L'abilitazione degli aggiornamenti gestiti della piattaforma garantisce l'installazione delle correzioni, degli aggiornamenti e delle funzionalità più recenti disponibili per l'ambiente. Mantenersi aggiornati sull'installazione delle patch è un passaggio importante per proteggere i sistemi.

Correzione

Per abilitare gli aggiornamenti gestiti della piattaforma, consulta Configurare gli aggiornamenti gestiti della piattaforma in Aggiornamenti gestiti della piattaforma nella Guida per gli AWS Elastic Beanstalk sviluppatori.

[ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch

Requisiti correlati: PCI DSS v4.0. 1/10.4.2, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Identificazione > Registrazione

Gravità: alta

Tipo di risorsa: `AWS::ElasticBeanstalk::Environment`

Regola AWS Config : `elastic-beanstalk-logs-to-cloudwatch`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`RetentionInDays`	Numero di giorni in cui conservare gli eventi di registro prima della scadenza	Enum	`1`, `3`, `5`, `7`, `14`, `30`, `60`, `90`, `120`, `150`, `180`, `365` , `400`, `545`, `731`, `1827`, `3653`	Nessun valore predefinito

Questo controllo verifica se un ambiente Elastic Beanstalk è configurato per inviare log a Logs. CloudWatch Il controllo fallisce se un ambiente Elastic Beanstalk non è configurato per inviare log a Logs. CloudWatch Facoltativamente, puoi fornire un valore personalizzato per il `RetentionInDays` parametro se desideri che il controllo passi solo se i log vengono conservati per il numero di giorni specificato prima della scadenza.

CloudWatch consente di raccogliere e monitorare varie metriche per le applicazioni e le risorse dell'infrastruttura. È inoltre possibile utilizzarlo CloudWatch per configurare le azioni di allarme in base a metriche specifiche. Ti consigliamo di integrare Elastic Beanstalk con per ottenere una maggiore visibilità nel tuo ambiente Elastic CloudWatch Beanstalk. I log di Elastic Beanstalk includono il file eb-activity.log, i log di accesso dall'ambiente nginx o dal server proxy Apache e i log specifici di un ambiente.

Correzione

Per integrare Elastic CloudWatch Beanstalk con Logs, consulta Streaming dei log delle istanze CloudWatch su Logs nella Developer Guide.AWS Elastic Beanstalk

Controlli CSPM di Security Hub per Elastic Load Balancing

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Elastic Load Balancing. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[ELB.1] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS

Requisiti correlati: PCI DSS v3.2. 1/2.3, PCI DSS v3.2. 1/4.1, 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) 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), profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Rilevamento > Servizi di rilevamento

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regola AWS Config : alb-http-to-https-redirection-check

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se il reindirizzamento da HTTP a HTTPS è configurato su tutti i listener HTTP di Application Load Balancers. Il controllo ha esito negativo se per uno dei listener HTTP di Application Load Balancers non è configurato il reindirizzamento da HTTP a HTTPS.

Prima di iniziare a utilizzare Application Load Balancer, è necessario aggiungere uno o più listener. Un listener è un processo che utilizza il protocollo e la porta configurati per verificare la presenza di richieste di connessione. I listener supportano entrambi i protocolli HTTP e HTTPS. È possibile utilizzare un listener HTTPS per affidare il lavoro di crittografia e decrittografia al sistema di bilanciamento del carico. Per applicare la crittografia in transito, è necessario utilizzare le azioni di reindirizzamento con Application Load Balancers per reindirizzare le richieste HTTP dei client a una richiesta HTTPS sulla porta 443.

Per ulteriori informazioni, consulta Listeners for your Application Load Balancers nella User Guide for Application Load Balancers.

Correzione

Per reindirizzare le richieste HTTP su HTTPS, è necessario aggiungere una regola listener Application Load Balancer o modificare una regola esistente.

Per istruzioni sull'aggiunta di una nuova regola, consulta Aggiungere una regola nella Guida utente di Application Load Balancers. Per Protocollo: Porta, scegliete HTTP, quindi immettete. **80** Per Aggiungi azione, Reindirizza a, scegli HTTPS, quindi inserisci**443**.

Per istruzioni sulla modifica di una regola esistente, consulta Modificare una regola nella Guida utente di Application Load Balancers. Per Protocollo: Porta, scegliete HTTP, quindi immettete. **80** Per Aggiungi azione, Reindirizza a, scegli HTTPS, quindi inserisci**443**.

[ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager

Requisiti correlati: 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 Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06, Profilo CRI v2. 2/PR. PS-01.07

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancing::LoadBalancer`

Regola AWS Config : elb-acm-certificate-required

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il Classic Load Balancer utilizza i HTTPS/SSL certificati forniti da AWS Certificate Manager (ACM). Il controllo fallisce se il Classic Load Balancer configurato con HTTPS/SSL listener non utilizza un certificato fornito da ACM.

Per creare un certificato, puoi utilizzare ACM o uno strumento che supporti i protocolli SSL e TLS, come OpenSSL. Security Hub CSPM consiglia di utilizzare ACM per creare o importare certificati per il sistema di bilanciamento del carico.

ACM si integra con Classic Load Balancers in modo da poter distribuire il certificato sul sistema di bilanciamento del carico. È inoltre necessario rinnovare automaticamente questi certificati.

Correzione

Per informazioni su come associare un SSL/TLS certificato ACM a un Classic Load Balancer, consulta AWS l'articolo del Knowledge Center Come posso associare un certificato SSL/TLS ACM a un Classic, Application o Network Load Balancer?

[ELB.3] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS

Requisiti correlati: 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),, (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 v4.0. NIST.800-171.r2 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancing::LoadBalancer`

Regola AWS Config : elb-tls-https-listeners-only

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i listener Classic Load Balancer sono configurati con il protocollo HTTPS o TLS per le connessioni front-end (da client a load balancer). Il controllo è applicabile se un Classic Load Balancer dispone di ascoltatori. Se il Classic Load Balancer non dispone di un listener configurato, il controllo non riporta alcun risultato.

Il controllo passa se i listener Classic Load Balancer sono configurati con TLS o HTTPS per le connessioni front-end.

Il controllo fallisce se il listener non è configurato con TLS o HTTPS per le connessioni front-end.

Prima di iniziare a utilizzare un sistema di bilanciamento del carico, è necessario aggiungere uno o più listener. Un listener è un processo che utilizza il protocollo e la porta configurati per verificare la presenza di richieste di connessione. I listener possono supportare sia HTTP che protocolli. HTTPS/TLS È necessario utilizzare sempre un listener HTTPS o TLS, in modo che il load balancer esegua il lavoro di crittografia e decrittografia in transito.

Correzione

Per risolvere questo problema, aggiorna i listener in modo che utilizzino il protocollo TLS o HTTPS.

Per trasformare tutti gli ascoltatori non conformi in ascoltatori TLS/HTTPS

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Seleziona il Classic Load Balancer.
4. Nella scheda Listeners (Listener), seleziona Edit (Modifica).
5. Per tutti i listener in cui Load Balancer Protocol non è impostato su HTTPS o SSL, modificate l'impostazione su HTTPS o SSL.
6. Per tutti i listener modificati, nella scheda Certificati, scegliete Cambia default.
7. Selezionare un certificato per Certificati ACM e IAM.
8. Scegliere Salva come predefinito.

9. Dopo aver aggiornato tutti i listener, scegliete Salva.

[ELB.4] Application Load Balancer deve essere configurato per eliminare le intestazioni http non valide

Requisiti correlati: NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/6.2.4, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Sicurezza di rete

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regola AWS Config : alb-http-drop-invalid-header-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo valuta se un Application Load Balancer è configurato per eliminare intestazioni HTTP non valide. Il controllo ha esito negativo se il valore di `routing.http.drop_invalid_header_fields.enabled` è impostato su. `false`

Per impostazione predefinita, gli Application Load Balancer non sono configurati per eliminare valori di intestazione HTTP non validi. La rimozione di questi valori di intestazione impedisce gli attacchi di desincronizzazione HTTP.

> **Note**
>
> Ti consigliamo di disabilitare questo controllo se ELB.12 è abilitato nel tuo account. Per ulteriori informazioni, consulta [ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa.

Correzione

Per risolvere questo problema, configura il sistema di bilanciamento del carico in modo da eliminare i campi di intestazione non validi.

Per configurare il load balancer in modo da eliminare i campi di intestazione non validi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Load Balancers (Sistemi di bilanciamento del carico).
3. Scegliete un Application Load Balancer.
4. Da Azioni, scegli Modifica attributi.
5. In Elimina campi di intestazione non validi, scegli Abilita.
6. Selezionare Salva.

[ELB.5] La registrazione di Application e Classic Load Balancers deve essere abilitata

Requisiti correlati: 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), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), CRI Profile v2. 2/DE. CM-03.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa:`AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regola AWS Config : elb-logging-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'Application Load Balancer e il Classic Load Balancer hanno la registrazione abilitata. Se lo è, il controllo fallisce. `access_logs.s3.enabled` `false`

Elastic Load Balancing fornisce log di accesso che acquisiscono informazioni dettagliate sulle richieste inviate al tuo load balancer. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server. Puoi utilizzare questi log per analizzare i modelli di traffico e risolvere i problemi che potresti incontrare.

Per ulteriori informazioni, consulta i registri di accesso per il tuo Classic Load Balancer nella Guida per l'utente dei Classic Load Balancer.

Correzione

Per abilitare i log di accesso, consulta la Fase 3: Configurazione dei log di accesso nella Guida utente per Application Load Balancers.

[ELB.6] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-03.01

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regola AWS Config : elb-deletion-protection-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'applicazione, un gateway o un Network Load Balancer ha la protezione da eliminazione abilitata. Il controllo ha esito negativo se la protezione da eliminazione è disattivata.

Abilita la protezione dall'eliminazione per proteggere l'applicazione, il gateway o il Network Load Balancer dall'eliminazione.

Correzione

Per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente, è possibile abilitare la protezione da eliminazione. Per impostazione predefinita, la protezione da eliminazioni è disabilitata nel sistema di bilanciamento del carico.

Se si abilita la protezione da eliminazione per il sistema di bilanciamento del carico, è necessario disabilitare la protezione da eliminazione prima di poter eliminare il sistema di bilanciamento del carico.

Per abilitare la protezione da eliminazione per un Application Load Balancer, vedere Protezione da eliminazione nella User Guide for Application Load Balancer. Per abilitare la protezione da

eliminazione per un Gateway Load Balancer, vedere Protezione da eliminazione nella Guida utente di Gateway Load Balancer. Per abilitare la protezione da eliminazione per un Network Load Balancer, vedere Protezione da eliminazione nella Guida dell'utente per Network Load Balancer.

[ELB.7] I Classic Load Balancer dovrebbero avere abilitato il drenaggio della connessione

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/PR. IR-03.01

Categoria: Recupero > Resilienza

Gravità: bassa

Tipo di risorsa: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config regola: `elb-connection-draining-enabled` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i Classic Load Balancer hanno abilitato il drenaggio della connessione.

L'abilitazione del drenaggio della connessione sui Classic Load Balancer garantisce che il sistema di bilanciamento del carico interrompa l'invio di richieste alle istanze che non registrano alcuna registrazione o che non sono funzionanti. Mantiene aperte le connessioni esistenti. Ciò è particolarmente utile per le istanze nei gruppi di Auto Scaling, per garantire che le connessioni non vengano interrotte bruscamente.

Correzione

Per abilitare il drenaggio della connessione sui Classic Load Balancer, consulta Configurare il drenaggio della connessione per Classic Load Balancer nella Guida dell'utente per Classic Load Balancer.

[ELB.8] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita che sia solida AWS Config Durata

Requisiti correlati: 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), (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 SC-8

NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancing::LoadBalancer`

Regola AWS Config : elb-predefined-security-policy-ssl-check

Tipo di pianificazione: modifica attivata

Parametri:

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01` (non personalizzabile)

Questo controllo verifica se i HTTPS/SSL listener Classic Load Balancer utilizzano la policy predefinita. `ELBSecurityPolicy-TLS-1-2-2017-01` Il controllo fallisce se i HTTPS/SSL listener Classic Load Balancer non lo utilizzano. `ELBSecurityPolicy-TLS-1-2-2017-01`

Una politica di sicurezza è una combinazione di protocolli SSL, cifrari e l'opzione Server Order Preference. Le politiche predefinite controllano i codici, i protocolli e gli ordini di preferenza da supportare durante le negoziazioni SSL tra un client e un sistema di bilanciamento del carico.

L'utilizzo `ELBSecurityPolicy-TLS-1-2-2017-01` può aiutarti a soddisfare gli standard di conformità e sicurezza che richiedono la disabilitazione di versioni specifiche di SSL e TLS. Per ulteriori informazioni, consulta Policy di sicurezza SSL predefinite per Classic Load Balancers nella Guida per l'utente di Classic Load Balancers.

Correzione

Per informazioni su come utilizzare la politica di sicurezza predefinita `ELBSecurityPolicy-TLS-1-2-2017-01` con un Classic Load Balancer, consulta Configure security settings in User Guide for Classic Load Balancer.

[ELB.9] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancing::LoadBalancer`

Regola AWS Config : elb-cross-zone-load-balancing-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il bilanciamento del carico tra zone è abilitato per i Classic Load Balancer (CLB). Il controllo fallisce se il bilanciamento del carico tra zone non è abilitato per un CLB.

Un nodo di bilanciamento del carico distribuisce il traffico solo tra le destinazioni registrate nella sua zona di disponibilità. Se il bilanciamento del carico tra zone è disabilitato, ogni nodo del sistema di bilanciamento del carico distribuisce il traffico solo tra le destinazioni registrate nella sua zona di disponibilità. Se il numero di destinazioni registrate non è lo stesso nelle zone di disponibilità, il traffico non verrà distribuito in modo uniforme e le istanze in una zona potrebbero finire per essere utilizzate in modo eccessivo rispetto alle istanze in un'altra zona. Con il bilanciamento del carico tra zone abilitato, ogni nodo di load balancer per Classic Load Balancer distribuisce le richieste in modo uniforme tra le istanze registrate in tutte le zone di disponibilità abilitate. Per i dettagli, consulta Cross-zone il bilanciamento del carico nella Elastic Load Balancing User Guide.

Correzione

Per abilitare il bilanciamento del carico tra zone in un Classic Load Balancer, consulta Abilita il bilanciamento del carico tra zone nella Guida utente per Classic Load Balancer.

[ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancing::LoadBalancer`

Regola AWS Config : clb-multiple-az

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`minAvailabilityZones`	Numero minimo di zone di disponibilità	Enum	`2, 3, 4, 5, 6`	`2`

Questo controllo verifica se un Classic Load Balancer è stato configurato per coprire almeno il numero specificato di zone di disponibilità (AZ). Il controllo fallisce se il Classic Load Balancer non copre almeno il numero specificato di AZ. A meno che non si fornisca un valore di parametro personalizzato per il numero minimo di AZ, Security Hub CSPM utilizza un valore predefinito di due AZ.

È possibile configurare un Classic Load Balancer per distribuire le richieste in entrata tra le istanze Amazon EC2 in una singola zona di disponibilità o più zone di disponibilità. Un Classic Load Balancer che non si estende su più zone di disponibilità non è in grado di reindirizzare il traffico verso destinazioni in un'altra zona di disponibilità se l'unica zona di disponibilità configurata non è disponibile.

Correzione

Per aggiungere zone di disponibilità a un Classic Load Balancer, consulta Aggiungere o rimuovere sottoreti per il Classic Load Balancer nella Guida utente per Classic Load Balancer.

[ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa

Requisiti correlati: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 PCI DSS v4.0. 1/6.2.4, Profilo CRI v2. 2/GV. OC-04.03, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Protezione > Protezione dei dati > Integrità dei dati

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regola AWS Config : alb-desync-mode-check

Tipo di pianificazione: modifica attivata

Parametri:

- `desyncMode`: `defensive, strictest` (non personalizzabile)

Questo controllo verifica se un Application Load Balancer è configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa. Il controllo fallisce se un Application Load Balancer non è configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa.

I problemi relativi a HTTP Desync possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della coda di richieste o della cache. A loro volta, queste vulnerabilità possono portare al furto di credenziali o all'esecuzione di comandi non autorizzati. Gli Application Load Balancer configurati con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa proteggono l'applicazione dai problemi di sicurezza che potrebbero essere causati da HTTP Desync.

Correzione

Per aggiornare la modalità di mitigazione della desincronizzazione di un Application Load Balancer, consulta la modalità di mitigazione Desync nella User Guide for Application Load Balancers.

[ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità

Requisiti correlati: 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), CRI Profile v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regola AWS Config : elbv2-multiple-az

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`minAvailabilityZones`	Numero minimo di zone di disponibilità	Enum	`2, 3, 4, 5, 6`	2

Questo controllo verifica se un Elastic Load Balancer V2 (Application, Network o Gateway Load Balancer) ha registrato istanze da almeno il numero specificato di zone di disponibilità (AZ). Il controllo fallisce se un Elastic Load Balancer V2 non ha istanze registrate almeno nel numero specificato di AZ. A meno che non si fornisca un valore di parametro personalizzato per il numero minimo di AZ, Security Hub CSPM utilizza un valore predefinito di due AZ.

Il servizio Elastic Load Balancing distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una o più zone di disponibilità. Elastic Load Balancing ridimensiona il load balancer di volta in volta, in quanto il traffico in ingresso varia nel corso del tempo. Si consiglia di configurare almeno due zone di disponibilità per garantire la disponibilità dei servizi, poiché Elastic Load Balancer sarà in grado di indirizzare il traffico verso un'altra zona di disponibilità se una non è disponibile. La configurazione di più zone di disponibilità contribuirà a eliminare la presenza di un unico punto di errore per l'applicazione.

Correzione

Per aggiungere una zona di disponibilità a un Application Load Balancer, consulta Availability Zones for your Application Load Balancer nella User Guide for Application Load Balancer. Per aggiungere una zona di disponibilità a un Network Load Balancer, consulta Network Load Balancer nella User Guide for Network Load Balancer. Per aggiungere una zona di disponibilità a un Gateway Load Balancer, vedere Create a Gateway Load Balancer nella Guida utente per Gateway Load Balancer.

[ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa

Requisiti correlati: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 PCI DSS v4.0. 1/6.2.4, Profilo CRI v2. 2/GV. OC-04.03, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Protezione > Protezione dei dati > Integrità dei dati

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancing::LoadBalancer`

Regola AWS Config : clb-desync-mode-check

Tipo di pianificazione: modifica attivata

Parametri:

- `desyncMode`: `defensive, strictest` (non personalizzabile)

Questo controllo verifica se un Classic Load Balancer è configurato con la modalità difensiva o la più rigorosa di mitigazione della desincronizzazione. Il controllo fallisce se il Classic Load Balancer non è configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa.

I problemi relativi a HTTP Desync possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della coda delle richieste o della cache. A loro volta, queste vulnerabilità possono portare al dirottamento delle credenziali o all'esecuzione di comandi non autorizzati. I Classic Load Balancer configurati con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa proteggono l'applicazione dai problemi di sicurezza che potrebbero essere causati da HTTP Desync.

Correzione

Per aggiornare la modalità di mitigazione della desincronizzazione su un Classic Load Balancer, consulta Modify desync mitigation mode nella User Guide for Classic Load Balancer.

[ELB.16] Application Load Balancers deve essere associato a un AWS WAF ACL Web

Requisiti correlati: NIST.800-53.r5 AC-4 (21), CRI Profile v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.03

Categoria: Proteggi > Servizi di protezione

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regola AWS Config : alb-waf-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un Application Load Balancer è associato a una lista di controllo degli accessi AWS WAF classica o AWS WAF Web (Web ACL). Il controllo fallisce se il `Enabled` campo per la AWS WAF configurazione è impostato su. `false`

AWS WAF è un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web e le API dagli attacchi. Con AWS WAF, puoi configurare un ACL Web, ovvero un insieme di regole che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili da te definite. Ti consigliamo di associare l'Application Load Balancer a AWS WAF un ACL Web per proteggerlo da attacchi dannosi.

Correzione

Per associare un Application Load Balancer a un ACL Web, consulta Associating or dissociating a Web ACL con una risorsa nella Developer Guide. AWS AWS WAF

[ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate

Requisiti correlati: 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), CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancingV2::Listener`

Regola AWS Config : elbv2-predefined-security-policy-ssl-check

Tipo di pianificazione: modifica attivata

Parametri:`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` (non personalizzabile)

Questo controllo verifica se il listener HTTPS per un Application Load Balancer o il listener TLS per un Network Load Balancer è configurato per crittografare i dati in transito utilizzando una politica di sicurezza consigliata. Il controllo ha esito negativo se il listener HTTPS o TLS per un load balancer non è configurato per utilizzare una politica di sicurezza consigliata.

Elastic Load Balancing utilizza una configurazione di negoziazione SSL, nota come policy di sicurezza, per negoziare le connessioni tra un client e un sistema di bilanciamento del carico. La politica di sicurezza specifica una combinazione di protocolli e cifrari. Il protocollo stabilisce una connessione sicura tra un client e un server. Un codice è un algoritmo di crittografia che utilizza chiavi di crittografia per creare un messaggio codificato. Durante il processo di negoziazione della connessione, il client e il sistema di bilanciamento del carico forniscono un elenco di crittografie e protocolli supportati, in ordine di preferenza. L'utilizzo di una politica di sicurezza consigliata per un sistema di bilanciamento del carico può aiutarti a soddisfare gli standard di conformità e sicurezza.

Correzione

Per informazioni sulle politiche di sicurezza consigliate e su come aggiornare i listener, consulta le seguenti sezioni delle guide utente di Elastic Load Balancing: Criteri di sicurezza per Application Load Balancer, Criteri di sicurezza per Network Load Balancer, Aggiornamento di un listener HTTPS per Application Load Balancer e Aggiornamento di un listener per Network Load Balancer.

[ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito

Requisiti correlati: CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancingV2::Listener`

Regola AWS Config : elbv2-listener-encryption-in-transit

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il listener di un Application Load Balancer o Network Load Balancer è configurato per utilizzare un protocollo sicuro per la crittografia dei dati in transito. Il controllo ha esito negativo se un listener Application Load Balancer non è configurato per utilizzare il protocollo HTTPS o un listener Network Load Balancer non è configurato per utilizzare il protocollo TLS.

Per crittografare i dati trasmessi tra un client e un sistema di bilanciamento del carico, i listener Elastic Load Balancer devono essere configurati per utilizzare i protocolli di sicurezza standard del settore: HTTPS per Application Load Balancers o TLS per Network Load Balancers. Altrimenti, i dati trasmessi tra un client e un sistema di bilanciamento del carico sono vulnerabili all'intercettazione, alla manomissione e all'accesso non autorizzato. L'uso di HTTPS o TLS da parte di un listener è in linea con le migliori pratiche di sicurezza e aiuta a garantire la riservatezza e l'integrità dei dati durante la trasmissione. Ciò è particolarmente importante per le applicazioni che gestiscono informazioni sensibili o che devono rispettare gli standard di sicurezza che richiedono la crittografia dei dati in transito.

Correzione

Per informazioni sulla configurazione dei protocolli di sicurezza per i listener, consulta le seguenti sezioni delle guide utente di Elastic Load Balancing: Crea un listener HTTPS per il tuo Application Load Balancer e Crea un listener per il tuo Network Load Balancer.

[ELB.21] I gruppi target di Application e Network Load Balancer devono utilizzare protocolli di controllo dello stato crittografati

Requisiti correlati: CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancingV2::TargetGroup`

Regola AWS Config : elbv2-targetgroup-healthcheck-protocol-encrypted

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il gruppo target per i controlli dello stato delle applicazioni e del bilanciamento del carico di rete utilizza un protocollo di trasporto crittografato. Il controllo ha esito negativo se il protocollo di controllo dello stato di salute non utilizza HTTPS. Questo controllo non è applicabile ai tipi di target Lambda.

I Load Balancer inviano richieste di controllo dello stato di salute ai target registrati per determinarne lo stato e indirizzare il traffico di conseguenza. Il protocollo di controllo dello stato di salute specificato nella configurazione del gruppo target determina come vengono eseguiti questi controlli. Quando i protocolli di controllo dello stato di salute utilizzano comunicazioni non crittografate come HTTP, le richieste e le risposte possono essere intercettate o manipolate durante la trasmissione. Ciò consente agli aggressori di ottenere informazioni sulla configurazione dell'infrastruttura, alterare i risultati dei controlli sanitari o condurre attacchi man-in-the-middle che influiscono sulle decisioni di routing. L'utilizzo di HTTPS per i controlli sanitari fornisce una comunicazione crittografata tra il sistema di bilanciamento del carico e i suoi obiettivi, proteggendo l'integrità e la riservatezza delle informazioni sullo stato di salute.

Correzione

Per configurare controlli di integrità crittografati per il tuo gruppo target di Application Load Balancer, consulta Aggiornare le impostazioni del controllo dello stato di un gruppo target di Application Load Balancer nella Elastic Load Balancing User Guide. Per configurare controlli di integrità crittografati per il tuo gruppo target Network Load Balancer, consulta Aggiornare le impostazioni del controllo dello stato di un gruppo target di Network Load Balancer nella Elastic Load Balancing User Guide.

[ELB.22] I gruppi target ELB devono utilizzare protocolli di trasporto crittografati

Requisiti correlati: CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancingV2::TargetGroup`

Regola AWS Config : elbv2-targetgroup-protocol-encrypted

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo target Elastic Load Balancing utilizza un protocollo di trasporto crittografato. Questo controllo non si applica ai gruppi target con un tipo di destinazione Lambda o ALB o ai gruppi target che utilizzano il protocollo GENEVE. Il controllo fallisce se il gruppo target non utilizza il protocollo HTTPS, TLS o QUIC.

La crittografia dei dati in transito li protegge dall'intercettazione da parte di utenti non autorizzati. I gruppi target che utilizzano protocolli non crittografati (HTTP, TCP, UDP) trasmettono i dati senza crittografia, rendendoli vulnerabili alle intercettazioni. L'utilizzo di protocolli crittografati (HTTPS, TLS, QUIC) garantisce la protezione dei dati trasmessi tra i sistemi di bilanciamento del carico e le destinazioni.

Correzione

Per utilizzare un protocollo crittografato, è necessario creare un nuovo gruppo target con il protocollo HTTPS, TLS o QUIC. Il protocollo del gruppo target non può essere modificato dopo la creazione. Per creare un gruppo target di Application Load Balancer, consulta Creare un gruppo target per il tuo Application Load Balancer nella Elastic Load Balancing User Guide. Per creare un gruppo target di Network Load Balancer, consulta Creare un gruppo target per il Network Load Balancer nella Elastic Load Balancing User Guide.

Security Hub CSPM per Elasticsearch

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Elasticsearch.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[ES.1] I domini Elasticsearch devono avere la crittografia a riposo abilitata

Requisiti correlati: PCI DSS v3.2. 1/3.4, 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), Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::Elasticsearch::Domain`

Regola AWS Config : `elasticsearch-encrypted-at-rest`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se nei domini Elasticsearch è abilitata la configurazione Encryption at Rest. Il controllo non riesce se la crittografia dei dati inattivi non è abilitata.

Per un ulteriore livello di sicurezza per i tuoi dati sensibili OpenSearch, dovresti configurarli in modo che vengano crittografati quando sono inattivi. OpenSearch I domini Elasticsearch offrono la crittografia dei dati archiviati. La funzionalità consente di AWS KMS archiviare e gestire le chiavi di crittografia. Per eseguire la crittografia, utilizza l'algoritmo Advanced Encryption Standard con chiavi a 256 bit ()AES-256.

Per ulteriori informazioni sulla OpenSearch crittografia a riposo, consulta Encryption of data at rest for Amazon OpenSearch Service nella Amazon OpenSearch Service Developer Guide.

Alcuni tipi di istanze, come `t.small` `et.medium`, non supportano la crittografia dei dati inattivi. Per i dettagli, consulta Tipi di istanze supportati nella Amazon OpenSearch Service Developer Guide.

Correzione

Per abilitare la crittografia a riposo per i domini Elasticsearch nuovi ed esistenti, consulta Enabling encryption of data at rest nella Amazon OpenSearch Service Developer Guide.

[ES.2] I domini Elasticsearch non devono essere accessibili al pubblico

Requisiti correlati: PCI DSS v3.2. 1/12.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 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), (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), NIST.800-53.r5 SC-7 PCI DSS versione 4.0. 1/1.4.4, Profilo CRI v2. 2/PR. IR-01.01

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Severità: critica

Tipo di risorsa: `AWS::Elasticsearch::Domain`

Regola AWS Config : `elasticsearch-in-vpc-only`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se i domini Elasticsearch si trovano in un VPC. Non valuta la configurazione del routing della sottorete VPC per determinare l'accesso pubblico. È necessario assicurarsi che i domini Elasticsearch non siano collegati a sottoreti pubbliche. Consulta Resource-basedle politiche nell'Amazon OpenSearch Service Developer Guide. È inoltre necessario assicurarsi che il VPC sia configurato in base alle procedure consigliate. Consulta le best practice di sicurezza per il tuo VPC nella Amazon VPC User Guide.

I domini Elasticsearch distribuiti all'interno di un VPC possono comunicare con le risorse VPC sulla rete AWS privata, senza la necessità di attraversare la rete Internet pubblica. Questa configurazione aumenta il livello di sicurezza limitando l'accesso ai dati in transito. I VPC forniscono una serie di controlli di rete per proteggere l'accesso ai domini Elasticsearch, inclusi ACL di rete e gruppi di sicurezza. Security Hub CSPM consiglia di migrare i domini Elasticsearch pubblici su VPC per sfruttare questi controlli.

Correzione

Se si crea un dominio con un endpoint pubblico, non è possibile inserirlo in un VPC in un secondo momento. Devi invece creare un nuovo dominio ed eseguire la migrazione dei dati. È vero anche il contrario. Se si crea un dominio all'interno di un VPC, non può avere un endpoint pubblico. È invece necessario creare un altro dominio o disabilitare questo controllo.

Consulta Lanciare i tuoi domini Amazon OpenSearch Service all'interno di un VPC nella Amazon OpenSearch Service Developer Guide.

[ES.3] I domini Elasticsearch devono crittografare i dati inviati tra i nodi

Requisiti correlati: 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. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. IR-01.05, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::Elasticsearch::Domain`

Regola AWS Config : `elasticsearch-node-to-node-encryption-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un dominio Elasticsearch ha la crittografia da nodo a nodo abilitata. Il controllo ha esito negativo se il dominio Elasticsearch non ha la crittografia da nodo a nodo abilitata. Il controllo produce risultati non riusciti anche se una versione di Elasticsearch non supporta i controlli di crittografia da nodo a nodo.

HTTPS (TLS) può essere utilizzato per impedire a potenziali aggressori di intercettare o manipolare il traffico di rete utilizzando attacchi person-in-the-middle o simili. Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS). L'abilitazione della crittografia da nodo a nodo per i domini Elasticsearch garantisce che le comunicazioni all'interno del cluster siano crittografate in transito.

Questa configurazione può comportare un calo delle prestazioni. È necessario conoscere e testare il compromesso in termini di prestazioni prima di attivare questa opzione.

Correzione

Per informazioni sull'attivazione della crittografia da nodo a nodo su domini nuovi ed esistenti, consulta Enabling node-to-node encryption nella Amazon Service Developer Guide. OpenSearch

[ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch

Requisiti correlati: 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), CRI NIST.800-53.r5 SI-7 Profile v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione - Registrazione

Gravità: media

Tipo di risorsa: `AWS::Elasticsearch::Domain`

Regola AWS Config : `elasticsearch-logs-to-cloudwatch`

Tipo di pianificazione: modifica attivata

Parametri:

- `logtype = 'error'`(non personalizzabile)

Questo controllo verifica se i domini Elasticsearch sono configurati per inviare log di errori a Logs. CloudWatch

È necessario abilitare i log degli errori per i domini Elasticsearch e inviarli a Logs per la conservazione e la risposta. CloudWatch I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

Correzione

Per informazioni su come abilitare la pubblicazione dei log, consulta Enabling log publishing (console) nella Amazon OpenSearch Service Developer Guide.

[ES.5] I domini Elasticsearch devono avere la registrazione di controllo abilitata

Requisiti correlati: 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), PCI NIST.800-53.r5 SI-7 DSS v4.0. 1/10.4.2, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::Elasticsearch::Domain`

AWS Config regola: `elasticsearch-audit-logging-enabled` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

- `cloudWatchLogsLogGroupArnList`(non personalizzabile). Security Hub CSPM non compila questo parametro. Comma-separated elenco di gruppi di CloudWatch log dei registri che devono essere configurati per i registri di controllo.

  Questa regola è valida `NON_COMPLIANT` se il gruppo di log CloudWatch Logs del dominio Elasticsearch non è specificato in questo elenco di parametri.

Questo controllo verifica se i domini Elasticsearch hanno la registrazione di controllo abilitata. Questo controllo ha esito negativo se un dominio Elasticsearch non ha la registrazione di controllo abilitata.

I log di controllo sono altamente personalizzabili. Ti consentono di tenere traccia delle attività degli utenti sui tuoi cluster Elasticsearch, inclusi i successi e gli errori di autenticazione, le richieste, le modifiche all' OpenSearchindice e le query di ricerca in arrivo.

Correzione

Per istruzioni dettagliate sull'abilitazione dei log di controllo, consulta Enabling audit logs nella Amazon OpenSearch Service Developer Guide.

[ES.6] I domini Elasticsearch devono avere almeno tre nodi di dati

Requisiti correlati: 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), CRI Profile v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::Elasticsearch::Domain`

AWS Config regola: `elasticsearch-data-node-fault-tolerance` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i domini Elasticsearch sono configurati con almeno tre nodi di dati e lo è. `zoneAwarenessEnabled` `true`

Un dominio Elasticsearch richiede almeno tre nodi di dati per un'elevata disponibilità e tolleranza agli errori. L'implementazione di un dominio Elasticsearch con almeno tre nodi di dati garantisce le operazioni del cluster in caso di guasto di un nodo.

Correzione

Per modificare il numero di nodi di dati in un dominio Elasticsearch

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/.
2. In Domini, scegli il nome del dominio che desideri modificare.
3. Scegli Modifica dominio.

4. In Nodi di dati, imposta Numero di nodi su un numero maggiore o uguale a `3`.

   Per tre implementazioni con zone di disponibilità, imposta un multiplo di tre per garantire una distribuzione equa tra le zone di disponibilità.

5. Seleziona Invia.

[ES.7] I domini Elasticsearch devono essere configurati con almeno tre nodi master dedicati

Requisiti correlati: 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), CRI Profile v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::Elasticsearch::Domain`

AWS Config regola: `elasticsearch-primary-node-fault-tolerance` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i domini Elasticsearch sono configurati con almeno tre nodi primari dedicati. Questo controllo ha esito negativo se il dominio non utilizza nodi primari dedicati. Questo controllo viene eseguito se i domini Elasticsearch hanno cinque nodi primari dedicati. Tuttavia, l'utilizzo di più di tre nodi primari potrebbe non essere necessario per mitigare il rischio di disponibilità e comportare costi aggiuntivi.

Un dominio Elasticsearch richiede almeno tre nodi primari dedicati per l'elevata disponibilità e la tolleranza agli errori. Le risorse dedicate dei nodi primari possono essere sovraccariche durante le blue/green implementazioni dei nodi dati perché ci sono nodi aggiuntivi da gestire. L'implementazione di un dominio Elasticsearch con almeno tre nodi primari dedicati garantisce una sufficiente capacità di risorse del nodo primario e operazioni del cluster in caso di guasto di un nodo.

Correzione

Per modificare il numero di nodi primari dedicati in un dominio OpenSearch

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/.

2. In Domini, scegli il nome del dominio che desideri modificare.
3. Scegli Modifica dominio.
4. In Nodi master dedicati, imposta il tipo di istanza sul tipo di istanza desiderato.
5. Imposta il numero di nodi master pari o superiore a tre.
6. Seleziona Invia.

[ES.8] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS

Requisiti correlati: 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), (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 SC-8 NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. IR-01.05, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::Elasticsearch::Domain`

AWS Config regola: `elasticsearch-https-required` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un endpoint del dominio Elasticsearch è configurato per utilizzare la politica di sicurezza TLS più recente. Il controllo fallisce se l'endpoint del dominio Elasticsearch non è configurato per utilizzare la politica supportata più recente o se HTTPS non è abilitato. L'ultima politica di sicurezza TLS attualmente supportata è. `Policy-Min-TLS-1-2-PFS-2023-10`

Puoi utilizzare HTTPS (TLS) per impedire a potenziali aggressori di utilizzare attacchi di tipo person-in-the-middle o simili per intercettare o manipolare traffico di rete. Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS). La crittografia dei dati in transito può influire sulle prestazioni. È consigliabile testare l'applicazione con questa funzionalità per comprendere il profilo delle prestazioni e l'impatto del TLS. TLS 1.2 offre diversi miglioramenti della sicurezza rispetto alle versioni precedenti di TLS.

Correzione

Per abilitare la crittografia TLS, utilizzate l'operazione UpdateDomainConfigAPI per configurare l'oggetto. DomainEndpointOptions Questo imposta il. `TLSSecurityPolicy`

[ES.9] I domini Elasticsearch devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Elasticsearch::Domain`

AWS Config regola: `tagged-elasticsearch-domain` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un dominio Elasticsearch ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il dominio non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il dominio non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un dominio Elasticsearch, consulta Working with tags nella Amazon OpenSearch Service Developer Guide.

Controlli CSPM del Security Hub per Amazon EMR

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse di Amazon EMR (precedentemente chiamato Amazon Elastic MapReduce). I controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici

Requisiti correlati: PCI DSS v3.2. 1/12.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 1/1.3.6, PCI DSS versione 4.0. 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), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: `AWS::EMR::Cluster`

AWS Config regola: emr-master-no-public-ip

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se i nodi master sui cluster Amazon EMR hanno indirizzi IP pubblici. Il controllo fallisce se gli indirizzi IP pubblici sono associati a una qualsiasi delle istanze del nodo master.

Gli indirizzi IP pubblici sono indicati nel `PublicIp` campo della `NetworkInterfaces` configurazione dell'istanza. Questo controllo controlla solo i cluster Amazon EMR che si trovano in uno `RUNNING` stato or. `WAITING`

Correzione

Durante l'avvio, puoi controllare se alla tua istanza in una sottorete predefinita o non predefinita viene assegnato un indirizzo IPv4 pubblico. Per impostazione predefinita, le sottoreti predefinite hanno questo attributo impostato su. `true` Le sottoreti non predefinite hanno l'attributo di indirizzamento pubblico IPv4 impostato su`false`, a meno che non sia stato creato dalla procedura guidata di avvio dell'istanza di Amazon EC2. In tal caso, l'attributo è impostato su. `true`

Dopo il lancio, non puoi dissociare manualmente un indirizzo IPv4 pubblico dalla tua istanza.

Per correggere un risultato non riuscito, è necessario avviare un nuovo cluster in un VPC con una sottorete privata con l'attributo di indirizzamento pubblico IPv4 impostato su. `false` Per istruzioni, consulta Launch clusters in un VPC nella Amazon EMR Management Guide.

[EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata

Requisiti correlati: 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), (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 NIST.800-53.r5 SC-7 (9), Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Gestione sicura degli accessi > Risorsa non accessibile al pubblico

Severità: critica

Tipo di risorsa: `AWS::::Account`

AWS Config regola: emr-block-public-access

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se il tuo account è configurato con l'accesso pubblico a blocchi di Amazon EMR. Il controllo fallisce se l'impostazione di blocco dell'accesso pubblico non è abilitata o se è consentita una porta diversa dalla porta 22.

L'accesso pubblico a blocchi di Amazon EMR impedisce l'avvio di un cluster in una sottorete pubblica se il cluster ha una configurazione di sicurezza che consente il traffico in entrata da indirizzi IP pubblici su una porta. Quando un utente dal tuo Account AWS avvia un cluster, Amazon EMR controlla le regole delle porte nel gruppo di sicurezza per il cluster e le confronta con le regole del traffico in entrata. Se il gruppo di sicurezza ha una regola in entrata che apre le porte agli indirizzi IP pubblici IPv4 0.0.0. 0/0 o IPv6: :/0, e tali porte non sono specificate come eccezioni per il tuo account, Amazon EMR non consente all'utente di creare il cluster.

> **Note**
>
> Il blocco dell'accesso pubblico è abilitato per impostazione predefinita. Per aumentare la protezione degli account, ti consigliamo di mantenerlo abilitato.

Correzione

Per configurare l'accesso pubblico a blocchi per Amazon EMR, consulta Using Amazon EMR block public access nella Amazon EMR Management Guide.

[EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CP-9 (8) NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::EMR::SecurityConfiguration`

Regola AWS Config : emr-security-configuration-encryption-rest

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una configurazione di sicurezza di Amazon EMR ha la crittografia a riposo abilitata. Il controllo fallisce se la configurazione di sicurezza non abilita la crittografia a riposo.

I dati inattivi si riferiscono ai dati archiviati in uno spazio di archiviazione persistente e non volatile per qualsiasi durata. La crittografia dei dati inutilizzati consente di proteggerne la riservatezza, riducendo il rischio che un utente non autorizzato possa accedervi.

Correzione

Per abilitare la crittografia a riposo in una configurazione di sicurezza di Amazon EMR, consulta Configurare la crittografia dei dati nella Amazon EMR Management Guide.

[EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito

Requisiti correlati: 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-23 (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::EMR::SecurityConfiguration`

Regola AWS Config : emr-security-configuration-encryption-transit

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una configurazione di sicurezza di Amazon EMR ha la crittografia in transito abilitata. Il controllo fallisce se la configurazione di sicurezza non abilita la crittografia in transito.

I dati in transito si riferiscono ai dati che si spostano da una posizione all'altra, ad esempio tra i nodi del cluster o tra il cluster e l'applicazione. I dati possono spostarsi su Internet o all'interno di una rete privata. La crittografia dei dati in transito riduce il rischio che un utente non autorizzato possa intercettare il traffico di rete.

Correzione

Per abilitare la crittografia in transito in una configurazione di sicurezza di Amazon EMR, consulta Configurare la crittografia dei dati nella Amazon EMR Management Guide.

Controlli CSPM Security Hub per EventBridge

Questi AWS Security Hub CSPM controlli valutano il EventBridge servizio e le risorse Amazon.

Questi controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[EventBridge.2] i bus EventBridge degli eventi devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Events::EventBus`

AWS Config regola: `tagged-events-eventbus` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	I tag fanno distinzione tra maiuscole e minuscole			

Questo controllo verifica se un bus di EventBridge eventi Amazon ha tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il bus degli eventi non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il bus di eventi non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un bus di EventBridge eventi, consulta i EventBridge tag Amazon nella Amazon EventBridge User Guide.

[EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata

Requisiti correlati: 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), (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. 1/10.3.1, Profilo CRI v2. 2/PR. AA-05.01

Categoria: Protezione > Gestione sicura degli accessi > Risorsa non accessibile al pubblico

Gravità: bassa

Tipo di risorsa: `AWS::Events::EventBus`

Regola AWS Config : custom-eventbus-policy-attached

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se a un bus di eventi EventBridge personalizzato Amazon è associata una policy basata sulle risorse. Questo controllo fallisce se il bus di eventi personalizzato non dispone di una politica basata sulle risorse.

Per impostazione predefinita, a un bus di eventi EventBridge personalizzato non è associata una policy basata sulle risorse. Ciò consente ai responsabili dell'account di accedere al bus degli eventi. Allegando una policy basata sulle risorse al bus degli eventi, è possibile limitare l'accesso al bus degli eventi a determinati account, nonché concedere intenzionalmente l'accesso alle entità in un altro account.

Correzione

Per allegare una policy basata sulle risorse a un bus di eventi EventBridge personalizzato, consulta Using resource-based policies for Amazon EventBridge nella Amazon User Guide. EventBridge

[EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-03.01

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::Events::Endpoint`

Regola AWS Config : `global-endpoint-event-replication-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la replica degli eventi è abilitata per un endpoint EventBridge globale Amazon. Il controllo fallisce se la replica degli eventi non è abilitata per un endpoint globale.

Gli endpoint globali aiutano a rendere tollerante l'applicazione. Regional-fault Innanzitutto, devi assegnare un controllo dell'integrità Amazon Route 53 all'endpoint. Quando viene avviato il failover, il controllo dello stato segnala uno stato «non integro». Entro pochi minuti dall'avvio del failover, tutti gli eventi personalizzati vengono instradati a un router di eventi nella Regione secondaria e vengono elaborati da tale router di eventi. Quando utilizzi endpoint globali, puoi abilitare la replica degli eventi. La replica degli eventi invia tutti gli eventi personalizzati ai router di eventi nelle Regioni primarie e secondarie utilizzando regole gestite. Si consiglia di abilitare la replica degli eventi durante la configurazione degli endpoint globali. La replica degli eventi consente di verificare la corretta configurazione degli endpoint globali. La replica degli eventi è necessaria per il ripristino automatico da un evento di failover. Se non hai abilitato la replica degli eventi, dovrai reimpostare manualmente il controllo di integrità della Route 53 su «integro» prima che gli eventi vengano reindirizzati alla regione principale.

> **Note**
>
> Se utilizzi bus di eventi personalizzati, avrai bisogno di un bus pari personalizzato in ogni regione con lo stesso nome e nello stesso account affinché il failover funzioni correttamente. L'abilitazione della replica degli eventi può aumentare i costi mensili. Per informazioni sui prezzi, consulta la pagina EventBridge dei prezzi di Amazon.

Correzione

Per abilitare la replica degli eventi per gli endpoint EventBridge globali, consulta Create a global endpoint nella Amazon EventBridge User Guide. Per la replica degli eventi, seleziona Replica degli eventi abilitata.

Controlli CSPM di Security Hub per Amazon Fraud Detector

Questi controlli CSPM di Security Hub valutano il servizio e le risorse di Amazon Fraud Detector.

Questi controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::FraudDetector::EntityType`

Regola AWS Config: `frauddetector-entity-type-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un tipo di entità Amazon Fraud Detector ha tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se il tipo di entità non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il tipo di entità non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un tipo di entità Amazon Fraud Detector (console)

1. Apri la console Amazon Fraud Detector all'indirizzo. https://console.aws.amazon.com/frauddetector
2. Nel pannello di navigazione, scegli Entità.
3. Seleziona un tipo di entità dall'elenco.
4. Nella sezione tag del tipo di entità, scegli Gestisci tag.
5. Scegli Aggiungi nuovo tag. Immettere una chiave e un valore per il tag. Ripeti l'operazione per ulteriori coppie chiave-valore.
6. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

[FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::FraudDetector::Label`

Regola AWS Config: `frauddetector-label-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un'etichetta Amazon Fraud Detector contiene tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se l'etichetta non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'etichetta non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per

ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un'etichetta Amazon Fraud Detector (console)

1. Apri la console Amazon Fraud Detector all'indirizzo. https://console.aws.amazon.com/frauddetector
2. Nel pannello di navigazione, scegli Etichette.
3. Seleziona un'etichetta dall'elenco.
4. Nella sezione etichette e tag, scegli Gestisci tag.
5. Scegli Aggiungi nuovo tag. Immettere una chiave e un valore per il tag. Ripeti l'operazione per ulteriori coppie chiave-valore.
6. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

[FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::FraudDetector::Outcome`

Regola AWS Config: `frauddetector-outcome-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un risultato di Amazon Fraud Detector presenta tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se il risultato non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il risultato non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un risultato di Amazon Fraud Detector (console)

1. Apri la console Amazon Fraud Detector all'indirizzo. https://console.aws.amazon.com/frauddetector
2. Nel riquadro di navigazione, scegli Risultati.
3. Seleziona un risultato dall'elenco.
4. Nella sezione dei tag dei risultati, scegli Gestisci tag.
5. Scegli Aggiungi nuovo tag. Immettere una chiave e un valore per il tag. Ripeti l'operazione per ulteriori coppie chiave-valore.
6. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

[FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::FraudDetector::Variable`

Regola AWS Config: `frauddetector-variable-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se una variabile Amazon Fraud Detector contiene tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se la variabile non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la variabile non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a una variabile Amazon Fraud Detector (console)

1. Apri la console Amazon Fraud Detector all'indirizzo. https://console.aws.amazon.com/frauddetector
2. Nel riquadro di navigazione, scegli Variabili.
3. Seleziona una variabile dall'elenco.
4. Nella sezione dei tag delle variabili, scegli Gestisci tag.

5. Scegli Aggiungi nuovo tag. Immettere una chiave e un valore per il tag. Ripeti l'operazione per ulteriori coppie chiave-valore.
6. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

Controlli CSPM del Security Hub per Amazon FSx

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon FSx. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi

Requisiti correlati: 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, Profilo CRI v2. 2/ID. AM-07.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::FSx::FileSystem`

Regola AWS Config : fsx-openzfs-copy-tags-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un file system Amazon FSx for OpenZFS è configurato per copiare i tag su backup e volumi. Il controllo fallisce se il file system OpenZFS non è configurato per copiare i tag su backup e volumi.

L'identificazione e l'inventario delle risorse IT sono un aspetto importante della governance e della sicurezza. I tag consentono di classificare AWS le risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Ciò è utile quando si dispone di molte risorse dello stesso tipo, in quanto è possibile identificare rapidamente una risorsa specifica in base ai tag che le sono stati assegnati.

Correzione

Per informazioni sulla configurazione di un file system FSx for OpenZFS per copiare i tag su backup e volumi, consulta Updating a file system nella Amazon FSx for OpenZFS User Guide.

[FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup

Requisiti correlati: NIST.800-53.r5 CP-9 NIST.800-53.r5 CM-8, CRI Profile v2. 2/ID. AM-02.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::FSx::FileSystem`

Regola AWS Config : fsx-lustre-copy-tags-to-backups

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un file system Amazon FSx for Lustre è configurato per copiare tag su backup e volumi. Il controllo fallisce se il file system Lustre non è configurato per copiare i tag su backup e volumi.

L'identificazione e l'inventario delle risorse IT sono un aspetto importante della governance e della sicurezza. I tag consentono di classificare AWS le risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Ciò è utile quando si dispone di molte risorse dello stesso tipo, in quanto è possibile identificare rapidamente una risorsa specifica in base ai tag che le sono stati assegnati.

Correzione

Per informazioni sulla configurazione di un file system FSx for Lustre per copiare i tag nei backup, consulta Copiare i backup all'interno dello stesso nella Guida per l'utente di Amazon Account AWS FSx for Lustre.

[FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ

Requisiti correlati: CRI Profile v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::FSx::FileSystem`

Regola AWS Config : fsx-openzfs-deployment-type-check

Tipo di pianificazione: periodica

Parametri: `deploymentTypes: MULTI_AZ_1` (non personalizzabile)

Questo controllo verifica se un file system Amazon FSx for OpenZFS è configurato per utilizzare il tipo di distribuzione con più zone di disponibilità ()Multi-AZ. Il controllo fallisce se il file system non è configurato per utilizzare il Multi-AZ tipo di distribuzione.

Amazon FSx for OpenZFS supporta diversi tipi di implementazione per i file system: Multi-AZ (HA), (HA) e Single-AZ Single-AZ (non HA). I tipi di implementazione offrono diversi livelli di disponibilità e durabilità. Multi-AZ I file system (HA) sono composti da una coppia di file server ad alta disponibilità (HA) distribuiti su due zone di disponibilità (AZ). Consigliamo di utilizzare il tipo di implementazione Multi-AZ (HA) per la maggior parte dei carichi di lavoro di produzione, grazie al modello di elevata disponibilità e durabilità che offre.

Correzione

Puoi configurare un file system Amazon FSx for OpenZFS per utilizzare il tipo di Multi-AZ distribuzione al momento della creazione del file system. Non è possibile modificare il tipo di distribuzione per un file system FSx for OpenZFS esistente.

Per informazioni sui tipi e sulle opzioni di implementazione per FSx for OpenZFS file system, consulta Disponibilità e durabilità per Amazon FSx for OpenZFS e Gestione delle risorse del file system nella Guida per l'utente di Amazon FSx for OpenZFS.

[FSx.4] I file system FSx for NetApp ONTAP devono essere configurati per l'implementazione Multi-AZ

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::FSx::FileSystem`

Regola AWS Config : fsx-ontap-deployment-type-check

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`deploymentTypes`	Un elenco di tipi di distribuzione da includere nella valutazione. Il controllo genera un `FAILED` risultato se un file system non è configurato per utilizzare un tipo di distribuzione specificato nell'elenco.	Enum	`MULTI_AZ_1` , `MULTI_AZ_2`	`MULTI_AZ_1` , `MULTI_AZ_2`

Questo controllo verifica se un file system Amazon FSx for NetApp ONTAP è configurato per utilizzare un tipo di distribuzione con più zone di disponibilità (Multi-AZ). Il controllo fallisce se il file system non è configurato per utilizzare un tipo di Multi-AZ distribuzione. Facoltativamente, è possibile specificare un elenco di tipi di distribuzione da includere nella valutazione.

Amazon FSx for NetApp ONTAP supporta diversi tipi di implementazione per i file system: Single-AZ 1, Single-AZ 2, Multi-AZ 1 e 2. Multi-AZ I tipi di implementazione offrono diversi livelli di disponibilità e durabilità. Consigliamo di utilizzare un tipo di Multi-AZ implementazione per la maggior parte dei carichi di lavoro di produzione, grazie al modello di elevata disponibilità e durabilità fornito dai tipi di Multi-AZ implementazione. Multi-AZ i file system supportano tutte le funzionalità di disponibilità e durabilità dei Single-AZ file system. Inoltre, sono progettati per fornire una disponibilità continua dei dati anche quando una zona di disponibilità (AZ) non è disponibile.

Correzione

Non puoi modificare il tipo di implementazione per un file system Amazon FSx for NetApp ONTAP esistente. Tuttavia, puoi eseguire il backup dei dati e quindi ripristinarli su un nuovo file system che utilizza un tipo di Multi-AZ distribuzione.

Per informazioni sui tipi e sulle opzioni di implementazione per i file system FSx for ONTAP, vedere Disponibilità, durabilità e opzioni di implementazione e Gestione dei file system nella Guida per l'utente di FSx for ONTAP.

[FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione

Requisiti correlati: CRI Profile v2. 2/GV. OC-04.03, Profilo CRI v2. 2/GV. RM-09.02, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::FSx::FileSystem`

Regola AWS Config : fsx-windows-deployment-type-check

Tipo di pianificazione: periodica

Parametri: `deploymentTypes: MULTI_AZ_1` (non personalizzabile)

Questo controllo verifica se un file system Amazon FSx for Windows File Server è configurato per utilizzare il tipo di distribuzione con più zone di disponibilità Multi-AZ (). Il controllo fallisce se il file system non è configurato per utilizzare il tipo di Multi-AZ distribuzione.

Amazon FSx for Windows File Server supporta due tipi di distribuzione per i file system Single-AZ: Multi-AZe. I tipi di implementazione offrono diversi livelli di disponibilità e durabilità. Single-AZ i file system sono composti da una singola istanza di file server Windows e da un set di volumi di storage all'interno di un'unica zona di disponibilità (AZ). Multi-AZ i file system sono composti da un cluster ad alta disponibilità di file server Windows distribuiti su due zone di disponibilità. Si consiglia di utilizzare il tipo di Multi-AZ implementazione per la maggior parte dei carichi di lavoro di produzione, grazie al modello di elevata disponibilità e durabilità che offre.

Correzione

Puoi configurare un file system Amazon FSx for Windows File Server per utilizzare Multi-AZ il tipo di distribuzione al momento della creazione del file system. Non è possibile modificare il tipo di distribuzione per un file system FSx for Windows File Server esistente.

Per informazioni sui tipi e sulle opzioni di distribuzione per i file system FSx for Windows File Server, consulta Disponibilità e durabilità Single-AZ : e file system Multi-AZ e Guida introduttiva ad Amazon FSx for Windows File Server nella Amazon FSx for Windows File Server User Guide.

Controlli CSPM Security Hub per Global Accelerator

Questi AWS Security Hub CSPM controlli valutano il AWS Global Accelerator servizio e le risorse.

Questi controlli potrebbero non essere disponibili tuttiRegioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::GlobalAccelerator::Accelerator`

AWS Configregola: `tagged-globalaccelerator-accelerator` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	`No default value`

Questo controllo verifica se un AWS Global Accelerator acceleratore dispone di tag con i tasti specifici definiti nel parametro. `requiredTagKeys` Il controllo fallisce se l'acceleratore non ha alcuna chiave tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'acceleratore non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse.

L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un acceleratore globale Global Accelerator, consulta la sezione Tagging in nella AWS Global Accelerator Developer Guide. AWS Global Accelerator

Controlli CSPM Security Hub per AWS Glue

Questi AWS Security Hub CSPM controlli valutano il AWS Glue servizio e le risorse. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Glue.1] AWS Glue i lavori devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Glue::Job`

AWS Config regola: `tagged-glue-job` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un AWS Glue job ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il lavoro non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il lavoro non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un AWS Glue lavoro, consulta i AWS tag AWS Glue nella Guida per l'AWS Glue utente.

[Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate

Requisiti correlati: CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::Glue::MLTransform`

Regola AWS Config : glue-ml-transform-encrypted-at-rest

Tipo di pianificazione: modifica attivata

Parametri: No

Questo controllo verifica se una trasformazione di AWS Glue machine learning è crittografata quando è inattiva. Il controllo fallisce se la trasformazione dell'apprendimento automatico non è crittografata a riposo.

I dati inattivi si riferiscono ai dati archiviati in uno storage persistente e non volatile per qualsiasi durata. La crittografia dei dati inutilizzati consente di proteggerne la riservatezza, riducendo il rischio che un utente non autorizzato possa accedervi.

Correzione

Per configurare la crittografia per le trasformazioni dell'apprendimento AWS Glue automatico, consulta Lavorare con le trasformazioni dell'apprendimento automatico nella Guida per l'utente.AWS Glue

[Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue

Requisiti correlati: 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, Profilo CRI v2. 2/PR. PS-02.03

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: `AWS::Glue::Job`

Regola AWS Config : glue-spark-job-supported-version

Tipo di pianificazione: modifica attivata

Parametri:`minimumSupportedGlueVersion`: `3.0` (non personalizzabile)

Questo controllo verifica se un job AWS Glue for Spark è configurato per l'esecuzione su una versione supportata di AWS Glue. Il controllo fallisce se il job Spark è configurato per l'esecuzione su una versione precedente alla versione minima supportata. AWS Glue

> **Note**
>
> Questo controllo genera anche una `FAILED` ricerca per un job AWS Glue for Spark se la proprietà AWS Glue version (`GlueVersion`) non esiste o è nulla nell'elemento di configurazione (CI) per il lavoro. In questi casi, la scoperta include la seguente annotazione:. `GlueVersion is null or missing in glueetl job configuration` Per risolvere questo tipo di `FAILED` ricerca, aggiungi la `GlueVersion` proprietà alla configurazione del lavoro. Per un elenco delle versioni e degli ambienti di runtime supportati, consulta AWS Glue Versioni nella Guida AWS Glue per l'utente.

L'esecuzione dei job AWS Glue Spark sulle versioni correnti di AWS Glue può ottimizzare le prestazioni, la sicurezza e l'accesso alle funzionalità più recenti di AWS Glue. Può anche aiutare a proteggere dalle vulnerabilità di sicurezza. Ad esempio, potrebbe essere rilasciata una nuova versione per fornire aggiornamenti di sicurezza, risolvere problemi o introdurre nuove funzionalità.

Correzione

Per informazioni sulla migrazione di un job Spark a una versione supportata di AWS Glue, consulta Migrating AWS Glue for Spark jobs nella Guida per l'utente.AWS Glue

Controlli CSPM Security Hub per Amazon GuardDuty

Questi AWS Security Hub CSPM controlli valutano il GuardDuty servizio e le risorse Amazon. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[GuardDuty.1] GuardDuty dovrebbe essere abilitato

Requisiti correlati: NIST.800-53.r5 AC-2 NIST.800-53.r5 AU-6 (12), NIST.800-53.r5 AU-6 (1), (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 NIST.800-53.r5 SA-15 (2), NIST.800-53.r5 SA-8 (8), NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SA-8 (21), (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 versione 3.2. 1/111.4, PCI DSS versione 4.0. 1/11.5.1, Profilo CRI v2. 2/DE. CM-01.01, Profilo CRI v2. 2/DE. CM-01.02, Profilo CRI v2. 2/DE. CM-01.03

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : guardduty-enabled-centralized

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se Amazon GuardDuty è abilitato nel tuo GuardDuty account e nella tua regione.

Si consiglia vivamente di abilitarlo GuardDuty in tutte le AWS regioni supportate. In questo modo è possibile GuardDuty generare informazioni su attività non autorizzate o insolite, anche nelle regioni che non vengono utilizzate attivamente. Ciò consente anche GuardDuty di monitorare CloudTrail eventi globali Servizi AWS come IAM.

Correzione

Per abilitarlo GuardDuty, consulta la sezione Guida introduttiva GuardDuty nella Amazon GuardDuty User Guide.

[GuardDuty.2] GuardDuty i filtri devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::GuardDuty::Filter`

AWS Config regola: `tagged-guardduty-filter` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un GuardDuty filtro Amazon ha tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il filtro non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il filtro non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un GuardDuty filtro, TagResourceconsulta Amazon GuardDuty API Reference.

[GuardDuty.3] Gli GuardDuty IPSets devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::GuardDuty::IPSet`

AWS Config regola: `tagged-guardduty-ipset` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un Amazon GuardDuty IPSet ha tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se l'IPSet non ha alcuna chiave di tag o se non ha

tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'IPSet non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un GuardDuty IPSet, consulta TagResourceAmazon GuardDuty API Reference.

[GuardDuty.4] i GuardDuty rilevatori devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::GuardDuty::Detector`

AWS Config regola: `tagged-guardduty-detector` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un GuardDuty rilevatore Amazon dispone di tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il rilevatore non dispone di chiavi tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se il rilevatore non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un GuardDuty rilevatore, consulta TagResourceAmazon GuardDuty API Reference.

[GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato

Requisiti correlati: CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::GuardDuty::Detector`

Regola AWS Config : guardduty-eks-protection-audit-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se GuardDuty EKS Audit Log Monitoring è abilitato. Per un account autonomo, il controllo fallisce se GuardDuty EKS Audit Log Monitoring è disabilitato nell'account. In un ambiente con più account, il controllo fallisce se l'account GuardDuty amministratore delegato o qualsiasi account membro associato non ha abilitato EKS Audit Log Monitoring.

In un ambiente con più account, il controllo genera risultati solo nell'account amministratore delegato GuardDuty . Solo l'amministratore delegato può abilitare o disabilitare la funzione EKS Audit Log Monitoring per gli account dei membri dell'organizzazione. GuardDuty gli account membri non possono modificare questa configurazione dai propri account. Questo controllo genera `FAILED` risultati se l' GuardDuty amministratore delegato ha un account membro sospeso che non ha abilitato GuardDuty EKS Audit Log Monitoring. Per ricevere un `PASSED` risultato, l'amministratore delegato deve dissociare questi account sospesi. GuardDuty

GuardDuty EKS Audit Log Monitoring ti aiuta a rilevare attività potenzialmente sospette nei cluster Amazon Elastic Kubernetes Service (Amazon EKS). Il monitoraggio dei log di audit EKS utilizza i log di audit di Kubernetes per acquisire le attività cronologiche degli utenti, delle applicazioni che utilizzano l'API Kubernetes e il piano di controllo (control-plane).

Correzione

Per abilitare GuardDuty EKS Audit Log Monitoring, consulta EKS Audit Log Monitoring nella Amazon GuardDuty User Guide.

[GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata

Requisiti correlati: PCI DSS v4.0. 1/115.5.1, Profilo CRI v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-01.01, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/DE. CM-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::GuardDuty::Detector`

Regola AWS Config : guardduty-lambda-protection-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la protezione GuardDuty Lambda è abilitata. Per un account autonomo, il controllo fallisce se GuardDuty Lambda Protection è disabilitata nell'account. In un ambiente con più account, il controllo fallisce se l'account GuardDuty amministratore delegato o qualsiasi account membro associato non ha la protezione Lambda abilitata.

In un ambiente con più account, il controllo genera risultati solo nell'account amministratore delegato. GuardDuty Solo l'amministratore delegato può abilitare o disabilitare la funzionalità Lambda Protection per gli account dei membri dell'organizzazione. GuardDuty gli account membro non possono modificare questa configurazione dai propri account. Questo controllo genera `FAILED` risultati se l' GuardDuty amministratore delegato ha un account membro sospeso che non ha la protezione GuardDuty Lambda abilitata. Per ricevere un `PASSED` risultato, l'amministratore delegato deve dissociare questi account sospesi. GuardDuty

GuardDuty Lambda Protection ti aiuta a identificare potenziali minacce alla sicurezza quando viene richiamata una AWS Lambda funzione. Dopo aver abilitato Lambda Protection, GuardDuty inizia a monitorare i registri delle attività di rete Lambda associati alle funzioni Lambda del tuo. Account AWS Quando viene richiamata una funzione Lambda e GuardDuty identifica traffico di rete sospetto che

indica la presenza di un codice potenzialmente dannoso nella funzione Lambda, genera un risultato. GuardDuty

Correzione

Per abilitare GuardDuty Lambda Protection, consulta Configuring Lambda Protection nella Amazon User Guide. GuardDuty

[GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato

Requisiti correlati: PCI DSS v4.0. 1/115.5.1, Profilo CRI v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/DE. CM-01.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rileva > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::GuardDuty::Detector`

Regola AWS Config : guardduty-eks-protection-runtime-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se GuardDuty EKS Runtime Monitoring con gestione automatizzata degli agenti è abilitato. Per un account autonomo, il controllo fallisce se GuardDuty EKS Runtime Monitoring con gestione automatizzata degli agenti è disabilitato nell'account. In un ambiente con più account, il controllo fallisce se l'account GuardDuty amministratore delegato o qualsiasi account membro associato non dispone di EKS Runtime Monitoring con la gestione automatizzata degli agenti abilitata.

In un ambiente con più account, il controllo genera risultati solo nell'account amministratore delegato GuardDuty . Solo l'amministratore delegato può abilitare o disabilitare la funzionalità EKS Runtime Monitoring con gestione automatizzata degli agenti per gli account dei membri dell'organizzazione. GuardDuty gli account membri non possono modificare questa configurazione dai propri account. Questo controllo genera `FAILED` risultati se l' GuardDuty amministratore delegato ha un account membro sospeso che non ha GuardDuty EKS Runtime Monitoring abilitato. Per ricevere un `PASSED` risultato, l'amministratore delegato deve dissociare questi account sospesi in. GuardDuty

EKS Protection in Amazon GuardDuty fornisce una copertura per il rilevamento delle minacce per aiutarti a proteggere i cluster Amazon EKS all'interno del tuo AWS ambiente. EKS Runtime Monitoring utilizza eventi a livello di sistema operativo per aiutarti a rilevare potenziali minacce nei nodi e nei contenitori EKS all'interno dei cluster EKS.

Correzione

Per abilitare EKS Runtime Monitoring con la gestione automatizzata degli agenti, consulta GuardDuty Enabling Runtime Monitoring nella Amazon GuardDuty User Guide.

[GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata

Requisiti correlati: CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/GV. OC-04.03, Profilo CRI v2. 2/GV. RM-09.02, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. DS-01.02, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/PR. PS-05.01, Profilo CRI v2. 2/RS. AN-07.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::GuardDuty::Detector`

Regola AWS Config : guardduty-malware-protection-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la protezione GuardDuty da malware è abilitata. Per un account autonomo, il controllo fallisce se la protezione GuardDuty da malware è disattivata nell'account. In un ambiente con più account, il controllo fallisce se l'account GuardDuty amministratore delegato o qualsiasi account membro associato non ha la protezione antimalware abilitata.

In un ambiente con più account, il controllo genera risultati solo nell'account amministratore delegato GuardDuty . Solo l'amministratore delegato può abilitare o disabilitare la funzionalità di protezione da malware per gli account dei membri dell'organizzazione. GuardDuty gli account membri non possono modificare questa configurazione dai propri account. Questo controllo genera `FAILED` risultati se l' GuardDuty amministratore delegato ha un account membro sospeso che non ha la protezione

GuardDuty antimalware abilitata. Per ricevere un `PASSED` risultato, l'amministratore delegato deve dissociare questi account sospesi. GuardDuty

GuardDuty Malware Protection for EC2 ti aiuta a rilevare la potenziale presenza di malware eseguendo la scansione dei volumi Amazon Elastic Block Store (Amazon EBS) collegati alle istanze Amazon Elastic Compute Cloud (Amazon EC2) e ai carichi di lavoro dei container. Malware Protection offre opzioni di scansione in cui puoi decidere se includere o escludere istanze EC2 e carichi di lavoro dei container specifici al momento della scansione. Fornisce inoltre la possibilità di conservare le istantanee dei volumi EBS collegati alle istanze EC2 o ai carichi di lavoro dei container nei tuoi account. GuardDuty Gli snapshot vengono conservati solo in caso di rilevamento di malware e di generazione di esiti della protezione da malware.

Correzione

Per abilitare GuardDuty Malware Protection for EC2, consulta Configuring GuardDuty-initiated malware scan nella Amazon GuardDuty User Guide.

[GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata

Requisiti correlati: PCI DSS v4.0. 1/115.5.1, Profilo CRI v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-01.01, Profilo CRI v2. 2/DE. CM-02.01, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::GuardDuty::Detector`

Regola AWS Config : guardduty-rds-protection-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la protezione GuardDuty RDS è abilitata. Per un account autonomo, il controllo fallisce se la protezione GuardDuty RDS è disattivata nell'account. In un ambiente con più account, il controllo ha esito negativo se l'account GuardDuty amministratore delegato o qualsiasi account membro associato non ha la protezione RDS abilitata.

In un ambiente con più account, il controllo genera risultati solo nell'account amministratore delegato. GuardDuty Solo l'amministratore delegato può abilitare o disabilitare la funzionalità di protezione

RDS per gli account dei membri dell'organizzazione. GuardDuty gli account membro non possono modificare questa configurazione dai propri account. Questo controllo genera `FAILED` risultati se l' GuardDuty amministratore delegato ha un account membro sospeso che non ha la protezione GuardDuty RDS abilitata. Per ricevere un `PASSED` risultato, l'amministratore delegato deve dissociare questi account sospesi in. GuardDuty

RDS Protection in GuardDuty analizza e profila l'attività di accesso RDS per potenziali minacce di accesso ai tuoi database Amazon Aurora (Aurora Edition e MySQL-Compatible Aurora Edition). PostgreSQL-Compatible La funzionalità consente di identificare comportamenti di accesso potenzialmente sospetti. La Protezione RDS non richiede un'infrastruttura aggiuntiva ed è progettata in modo da non influire negativamente sulle prestazioni delle istanze di database. Quando RDS Protection rileva un tentativo di accesso potenzialmente sospetto o anomalo che indica una minaccia per il database, GuardDuty genera una nuova scoperta con dettagli sul database potenzialmente compromesso.

Correzione

Per abilitare GuardDuty RDS Protection, consulta GuardDuty RDS Protection nella Amazon GuardDuty User Guide.

[GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata

Requisiti correlati: PCI DSS v4.0. 1/115.5.1, Profilo CRI v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.01, Profilo CRI v2. 2/DE. CM-02.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::GuardDuty::Detector`

Regola AWS Config : guardduty-s3-protection-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se GuardDuty S3 Protection è abilitato. Per un account autonomo, il controllo fallisce se GuardDuty S3 Protection è disabilitato nell'account. In un ambiente con più

account, il controllo fallisce se l'account GuardDuty amministratore delegato o qualsiasi account membro associato non ha S3 Protection abilitato.

In un ambiente con più account, il controllo genera risultati solo nell'account amministratore delegato. GuardDuty Solo l'amministratore delegato può abilitare o disabilitare la funzionalità di protezione S3 per gli account membro dell'organizzazione. GuardDuty gli account membro non possono modificare questa configurazione dai propri account. Questo controllo genera `FAILED` risultati se l' GuardDuty amministratore delegato ha un account membro sospeso che non ha la protezione GuardDuty S3 abilitata. Per ricevere un `PASSED` risultato, l'amministratore delegato deve dissociare questi account sospesi in. GuardDuty

S3 Protection consente di monitorare le operazioni API GuardDuty a livello di oggetto per identificare potenziali rischi per la sicurezza dei dati all'interno dei bucket Amazon Simple Storage Service (Amazon S3). GuardDuty monitora le minacce contro le tue risorse S3 AWS CloudTrail analizzando gli eventi di gestione e gli eventi relativi ai dati S3. CloudTrail

Correzione

Per abilitare GuardDuty S3 Protection, consulta Amazon S3 Protection in Amazon nella GuardDuty GuardDuty Amazon User Guide.

[GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato

Requisiti correlati: CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-01.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rileva > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::GuardDuty::Detector`

Regola AWS Config : guardduty-runtime-monitoring-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se il Runtime Monitoring è abilitato in Amazon GuardDuty. Per un account autonomo, il controllo fallisce se il GuardDuty Runtime Monitoring è disabilitato per l'account. In un ambiente con più account, il controllo fallisce se il GuardDuty Runtime Monitoring è disabilitato per l'account GuardDuty amministratore delegato o per qualsiasi account membro associato.

In un ambiente con più account, solo l' GuardDuty amministratore delegato può abilitare o disabilitare il monitoraggio del GuardDuty runtime per gli account della propria organizzazione. Inoltre, solo l' GuardDuty amministratore può configurare e gestire gli agenti di sicurezza GuardDuty utilizzati per il monitoraggio in fase di esecuzione dei AWS carichi di lavoro e delle risorse per gli account dell'organizzazione. GuardDuty gli account dei membri non possono abilitare, configurare o disabilitare il monitoraggio del runtime per i propri account.

GuardDuty Runtime Monitoring osserva e analizza gli eventi a livello di sistema operativo, di rete e di file per aiutarti a rilevare potenziali minacce in carichi di AWS lavoro specifici del tuo ambiente. Utilizza agenti GuardDuty di sicurezza che aggiungono visibilità al comportamento di runtime, come l'accesso ai file, l'esecuzione dei processi, gli argomenti della riga di comando e le connessioni di rete. Puoi abilitare e gestire l'agente di sicurezza per ogni tipo di risorsa che desideri monitorare per rilevare potenziali minacce, come i cluster Amazon EKS e le istanze Amazon EC2.

Correzione

Per informazioni sulla configurazione e l'abilitazione del monitoraggio del GuardDuty runtime, consulta GuardDuty Runtime Monitoring e Enabling GuardDuty Runtime Monitoring nella Amazon GuardDuty User Guide.

[GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato

Requisiti correlati: CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/DE. CM-01.01, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rileva > Servizi di rilevamento

Gravità: media

Tipo di risorsa: `AWS::GuardDuty::Detector`

Regola AWS Config : guardduty-ecs-protection-runtime-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se l'agente di sicurezza GuardDuty automatizzato di Amazon è abilitato per il monitoraggio in fase di esecuzione dei cluster Amazon ECS su. AWS Fargate Per un account

autonomo, il controllo fallisce se il security agent è disabilitato per l'account. In un ambiente con più account, il controllo fallisce se il security agent è disabilitato per l'account GuardDuty amministratore delegato o per qualsiasi account membro associato.

In un ambiente con più account, questo controllo genera risultati solo nell'account amministratore delegato GuardDuty . Questo perché solo l' GuardDuty amministratore delegato può abilitare o disabilitare il monitoraggio in fase di esecuzione delle ECS-Fargate risorse per gli account della propria organizzazione. GuardDuty gli account dei membri non possono eseguire questa operazione per i propri account. Inoltre, questo controllo genera `FAILED` risultati se GuardDuty è sospeso per un account membro e il monitoraggio in fase di esecuzione delle ECS-Fargate risorse è disabilitato per l'account membro. Per ricevere un `PASSED` risultato, l' GuardDuty amministratore deve dissociare l'account membro sospeso dal proprio account amministratore utilizzando GuardDuty.

GuardDuty Runtime Monitoring osserva e analizza gli eventi a livello di sistema operativo, di rete e di file per aiutarti a rilevare potenziali minacce in carichi di lavoro specifici AWS dell'ambiente. Utilizza agenti GuardDuty di sicurezza che aggiungono visibilità al comportamento di runtime, come l'accesso ai file, l'esecuzione dei processi, gli argomenti della riga di comando e le connessioni di rete. È possibile abilitare e gestire il security agent per ogni tipo di risorsa che si desidera monitorare per rilevare potenziali minacce. Ciò include i cluster Amazon ECS attivi. AWS Fargate

Correzione

Per abilitare e gestire l'agente di sicurezza per il monitoraggio in fase di GuardDuty esecuzione delle ECS-Fargate risorse, è necessario GuardDuty utilizzarlo direttamente. Non è possibile abilitarlo o gestirlo manualmente per ECS-Fargate le risorse. Per informazioni sull'attivazione e la gestione del security agent, consulta Prerequisiti per il supporto AWS Fargate (solo Amazon ECS) e Gestione dell'agente di sicurezza automatizzato per (solo AWS Fargate Amazon ECS) nella Amazon GuardDuty User Guide.

[GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato

Requisiti correlati: CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.01, Profilo CRI v2. 2/DE. CM-01.01, Profilo CRI v2. 2/DE. CM-03.02

Categoria: Rileva > Servizi di rilevamento

Gravità: media

Tipo di risorsa: `AWS::GuardDuty::Detector`

Regola AWS Config : guardduty-ec2-protection-runtime-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se l'agente di sicurezza GuardDuty automatizzato di Amazon è abilitato per il monitoraggio del runtime delle istanze Amazon EC2. Per un account autonomo, il controllo fallisce se il security agent è disabilitato per l'account. In un ambiente con più account, il controllo fallisce se il security agent è disabilitato per l'account GuardDuty amministratore delegato o per qualsiasi account membro associato.

In un ambiente con più account, questo controllo genera risultati solo nell'account amministratore delegato GuardDuty . Questo perché solo l' GuardDuty amministratore delegato può abilitare o disabilitare il monitoraggio del runtime delle istanze Amazon EC2 per gli account della propria organizzazione. GuardDuty gli account dei membri non possono eseguire questa operazione per i propri account. Inoltre, questo controllo genera `FAILED` risultati se GuardDuty è sospeso per un account membro e il monitoraggio del runtime delle istanze EC2 è disabilitato per l'account membro. Per ricevere un `PASSED` risultato, l' GuardDuty amministratore deve dissociare l'account membro sospeso dal proprio account amministratore utilizzando. GuardDuty

GuardDuty Runtime Monitoring osserva e analizza gli eventi a livello di sistema operativo, di rete e di file per aiutarti a rilevare potenziali minacce in carichi di lavoro specifici AWS dell'ambiente. Utilizza agenti GuardDuty di sicurezza che aggiungono visibilità al comportamento di runtime, come l'accesso ai file, l'esecuzione dei processi, gli argomenti della riga di comando e le connessioni di rete. È possibile abilitare e gestire il security agent per ogni tipo di risorsa che si desidera monitorare per rilevare potenziali minacce. Sono incluse le istanze Amazon EC2.

Correzione

Per informazioni sulla configurazione e la gestione dell'agente di sicurezza automatizzato per il monitoraggio del GuardDuty runtime delle istanze EC2, consulta Prerequisiti per il supporto delle istanze Amazon EC2 e Abilitazione dell'agente di sicurezza automatizzato per le istanze Amazon EC2 nella Amazon User Guide. GuardDuty

Controlli CSPM Security Hub per AWS Identity and Access Management

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse AWS Identity and Access Management (IAM). I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/1.22, benchmark AWS CIS 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, (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 3.1.4, PCI DSS versione 3.2. 1/7.2.1, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: alta

Tipo di risorsa: `AWS::IAM::Policy`

Regola AWS Config : `iam-policy-no-statements-with-admin-access`

Tipo di pianificazione: modifica attivata

Parametri:

- `excludePermissionBoundaryPolicy: true`(non personalizzabile)

Questo controllo verifica se la versione predefinita delle politiche IAM (note anche come politiche gestite dai clienti) dispone dell'accesso come amministratore includendo un'istruzione `"Effect": "Allow"` con `"Action": "*"` over`"Resource": "*"`. Il controllo fallisce se si dispone di politiche IAM con una dichiarazione di questo tipo.

Il controllo verifica solo le policy gestite dal cliente create dall'utente. Non verifica le politiche in linea e AWS gestite.

Le politiche IAM definiscono una serie di privilegi concessi a utenti, gruppi o ruoli. Seguendo i consigli di sicurezza standard, si AWS consiglia di concedere il privilegio minimo, il che significa concedere solo le autorizzazioni necessarie per eseguire un'attività. Quando si forniscono privilegi amministrativi completi anziché il set di autorizzazioni minimo di cui l'utente ha bisogno, si espongono le risorse a operazioni potenzialmente indesiderate.

Anziché consentire privilegi di amministratore completi, determina ciò che gli utenti devono fare e crea le policy su misura che permettono agli utenti di eseguire solo tali attività. È più sicuro iniziare con un set di autorizzazioni minimo e concedere autorizzazioni aggiuntive quando necessario. Non iniziare con autorizzazioni troppo permissive e cercare di limitarle in un secondo momento.

È necessario rimuovere le policy IAM che hanno una dichiarazione `"Effect": "Allow"` con `"Action": "*"` over. `"Resource": "*"`

> **Note**
>
> AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub CSPM. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per modificare le policy IAM in modo che non consentano i privilegi amministrativi «*» completi, consulta Modifica delle policy IAM nella IAM User Guide.

[IAM.2] Gli utenti IAM non devono avere policy IAM allegate

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.14, benchmark AWS CIS Foundations v3.0. 0/1.15, benchmark AWS CIS 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 (3), NIST.800-171.r2 3.1.1, NIST.800-171.r2 3.1.2 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 NIST.800-171.r2 3.1.7, 3.3.9, 3.13.3, PCI DSS versione 3.2. NIST.800-171.r2 NIST.800-171.r2 1/7.2.1, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: `AWS::IAM::User`

Regola AWS Config : `iam-user-no-policies-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se gli utenti IAM hanno delle policy allegate. Il controllo fallisce se gli utenti IAM hanno delle policy allegate. Gli utenti IAM devono invece ereditare le autorizzazioni dai gruppi IAM o assumere un ruolo.

Per impostazione predefinita, gli utenti, i gruppi e i ruoli IAM non hanno accesso alle AWS risorse. Le policy IAM concedono privilegi a utenti, gruppi o ruoli. Ti consigliamo di applicare le policy IAM direttamente ai gruppi e ai ruoli ma non agli utenti. L'assegnazione di privilegi a livello di gruppo o ruolo riduce la complessità di gestione degli accessi, se il numero di utenti cresce. La riduzione della complessità di gestione degli accessi potrebbe a sua volta ridurre l'opportunità per un principale di ricevere o mantenere inavvertitamente privilegi eccessivi.

> **Note**
>
> AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub CSPM. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola regione, è possibile disabilitare questo controllo in tutte le regioni tranne la regione in cui si registrano le risorse globali.

Correzione

Per risolvere questo problema, crea un gruppo IAM e allega la policy al gruppo. Quindi, aggiungi gli utenti al gruppo. La policy viene applicata a ogni utente nel gruppo. Per rimuovere una policy collegata direttamente a un utente, consulta Aggiungere e rimuovere le autorizzazioni di identità IAM nella Guida per l'utente IAM.

[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.13, benchmark AWS CIS Foundations v3.0. 0/1.14, benchmark AWS CIS Foundations v1.4. 0/1.14, benchmark AWS CIS 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 versione 4.0. 1/83.3.9, PCI DSS versione 4.0. 1/8.6.3, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-05.03

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::IAM::User`

Regola AWS Config : `access-keys-rotated`

Tipo di pianificazione: periodica

Parametri:

- `maxAccessKeyAge`: `90` (non personalizzabile)

Questo controllo verifica se le chiavi di accesso attive vengono ruotate entro 90 giorni.

Ti consigliamo vivamente di non generare e rimuovere tutte le chiavi di accesso nell'account. Invece, la best practice consigliata consiste nel creare uno o più ruoli IAM o utilizzare la federazione tramite Centro identità AWS IAM. Puoi utilizzare questi metodi per consentire agli utenti di accedere a Console di gestione AWS e AWS CLI.

Ogni approccio ha i suoi casi d'uso. La federazione è generalmente la soluzione migliore per le aziende che dispongono di una directory centrale esistente o che prevedono di aver bisogno di più del limite attuale per gli utenti IAM. Le applicazioni eseguite all'esterno di un AWS ambiente necessitano di chiavi di accesso per l'accesso programmatico alle AWS risorse.

Tuttavia, se le risorse che richiedono l'accesso programmatico vengono eseguite all'interno AWS, la migliore pratica consiste nell'utilizzare i ruoli IAM. I ruoli consentono di concedere l'accesso a una risorsa senza codificare l'ID chiave di accesso e la chiave di accesso segreta nella configurazione.

Per ulteriori informazioni sulla protezione delle chiavi di accesso e dell'account, consulta le migliori pratiche per la gestione delle chiavi di AWS accesso nel Riferimenti generali di AWS. Consulta anche il post del blog Linee guida per proteggere l'utente Account AWS durante l'utilizzo dell'accesso programmatico.

Se disponi già di una chiave di accesso, Security Hub CSPM consiglia di ruotare le chiavi di accesso ogni 90 giorni. La rotazione delle chiavi di accesso riduce la possibilità di utilizzo di una chiave di accesso associata a un account compromesso o chiuso. Garantisce inoltre che i dati non possano essere accessibili con una vecchia chiave che potrebbe essere stata persa, decifrata o rubata. Aggiorna sempre le applicazioni dopo aver ruotato le chiavi di accesso.

Le chiavi di accesso sono composte da un ID chiave di accesso e una chiave di accesso segreta. Vengono utilizzate per firmare le richieste programmatiche inviate dall'utente. AWS Gli utenti hanno bisogno delle proprie chiavi di accesso per effettuare chiamate programmatiche AWS da Tools for Windows PowerShell, dagli AWS SDK o chiamate HTTP dirette utilizzando le operazioni API per singoli utenti. AWS CLI Servizi AWS

Se la tua organizzazione utilizza Centro identità AWS IAM (IAM Identity Center), i tuoi utenti possono accedere ad Active Directory, a una directory IAM Identity Center integrata o a un altro provider di

identità (IdP) connesso a IAM Identity Center. Possono quindi essere mappati su un ruolo IAM che consente loro di eseguire AWS CLI comandi o richiamare operazioni AWS API senza la necessità di chiavi di accesso. Per ulteriori informazioni, consulta Configurazione dell'uso Centro identità AWS IAM nella Guida AWS CLI per l'AWS Command Line Interface utente.

> **Note**
>
> AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub CSPM. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per ruotare le chiavi di accesso più vecchie di 90 giorni, consulta Rotating access keys nella IAM User Guide. Segui le istruzioni per qualsiasi utente con una chiave di accesso di età superiore a 90 giorni.

[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.3, benchmark AWS CIS Foundations v3.0. 0/1.4, benchmark AWS CIS Foundations v1.4. 0/1.4, benchmark AWS CIS Foundations v1.2. 0/1.12, PCI DSS versione 3.2. 1/2.1, PCI DSS versione 3.2. 1/2.2, PCI DSS versione 3.2. 1/7.2.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), (7), NIST.800-53.r5 AC-3 (10) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (2), profilo CRI NIST.800-53.r5 AC-6 v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. AA-05.02

Categoria: Protezione > Gestione degli accessi sicuri

Severità: critica

Tipo di risorsa: `AWS:::Account`

Regola AWS Config : `iam-root-access-key-check`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se è presente la chiave di accesso dell'utente root.

L'utente root è l'utente con più privilegi in un Account AWS. AWS le chiavi di accesso forniscono l'accesso programmatico a un determinato account.

Security Hub CSPM consiglia di rimuovere tutte le chiavi di accesso associate all'utente root. Ciò limita i vettori che possono essere utilizzati per compromettere l'account. Incoraggia inoltre la creazione e l'utilizzo di account basati sul ruolo che dispongono di meno privilegi.

Correzione

Per eliminare la chiave di accesso dell'utente root, consulta Eliminazione delle chiavi di accesso per l'utente root nella IAM User Guide. Per eliminare le chiavi di accesso dell'utente root da un Account AWS ingresso AWS GovCloud (US), consulta Eliminazione delle chiavi di accesso dell'utente root del mio AWS GovCloud (US) account nella Guida per l'AWS GovCloud (US) utente.

[IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.9, benchmark AWS CIS Foundations v3.0. 0/1.10, benchmark AWS CIS Foundations v1.4. 0/1.10, benchmark AWS CIS Foundations v1.2. 0/1.2, 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 versione 4.0. 1/8.4.2, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-05.02

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::IAM::User`

Regola AWS Config : `mfa-enabled-for-iam-console-access`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se l' AWS autenticazione a più fattori (MFA) è abilitata per tutti gli utenti IAM che utilizzano una password della console.

Multi-factor l'autenticazione (MFA) aggiunge un ulteriore livello di protezione oltre a nome utente e password. Con l'MFA abilitata, quando un utente accede a un AWS sito Web, gli vengono richiesti

il nome utente e la password. Inoltre, viene richiesto loro un codice di autenticazione dal dispositivo AWS MFA.

Ti consigliamo di abilitare MFA per tutti gli account che dispongono di una password della console. MFA è progettato per fornire una maggiore sicurezza per l'accesso alla console. L'entità principal di autenticazione deve possedere un dispositivo che genera una chiave legata al fattore tempo e deve essere a conoscenza delle credenziali.

> **Note**
>
> AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub CSPM. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per aggiungere MFA per gli utenti IAM, consulta Using Multi-Factor Authentication (MFA) AWS nella IAM User Guide.

[IAM.6] La MFA hardware deve essere abilitata per l'utente root

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.5, benchmark AWS CIS Foundations v3.0. 0/1.6, benchmark AWS CIS Foundations v1.4. 0/1.6, benchmark AWS CIS Foundations v1.2. 0/1.14, PCI DSS versione 3.2. 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 versione 4.0. 1/8.4.2, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-05.02

Categoria: Protezione > Gestione degli accessi sicuri

Severità: critica

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `root-account-hardware-mfa-enabled`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se l'utente Account AWS è abilitato a utilizzare un dispositivo hardware di autenticazione a più fattori (MFA) per accedere con le credenziali dell'utente root. Il controllo fallisce se l'autenticazione MFA hardware non è abilitata o se i dispositivi MFA virtuali sono autorizzati ad accedere con le credenziali dell'utente root.

Di conseguenza, un dispositivo MFA virtuale potrebbe non offrire lo stesso livello di sicurezza di un dispositivo hardware MFA. Ti consigliamo di utilizzare un dispositivo MFA virtuale solo in attesa dell'approvazione dell'acquisto dell'hardware o dell'arrivo dell'hardware. Per saperne di più, consulta Assegnare un dispositivo MFA virtuale (console) nella Guida per l'utente IAM.

> **Note**
>
> Security Hub CSPM valuta questo controllo in base alla presenza di credenziali utente root (profilo di accesso) in un. Account AWS Il controllo genera `PASSED` risultati nei seguenti casi:
>
> - Le credenziali dell'utente root sono presenti nell'account e la MFA hardware è abilitata per l'utente root.
> - Le credenziali dell'utente root non sono presenti nell'account.
>
> Il controllo genera un `FAILED` risultato se le credenziali dell'utente root sono presenti nell'account e la MFA hardware non è abilitata per l'utente root.

Correzione

Per informazioni sull'attivazione della MFA hardware per l'utente root, consulta la sezione Multi-factor authentication for an Utente root dell'account AWS nella IAM User Guide.

[IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide

Requisiti correlati: 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, 3.5.8, PCI DSS NIST.800-171.r2 v4.0. 1/83.3.6, PCI DSS versione 4.0. 1/8.3.7, PCI DSS versione 4.0. 1/8.3.9, PCI DSS versione 4.0. 1/83.10.1, PCI DSS versione 4.0. 1/8.6.3, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-05.02

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `iam-password-policy`

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`RequireUppercaseCharacters`	Richiede almeno un carattere maiuscolo nella password	Booleano	`true` o `false`	`true`
`RequireLowercaseCharacters`	Richiede almeno un carattere minuscolo nella password	Booleano	`true` o `false`	`true`
`RequireSymbols`	Richiedi almeno un simbolo nella password	Booleano	`true` o `false`	`true`
`RequireNumbers`	Richiedi almeno un numero nella password	Booleano	`true` o `false`	`true`
`MinimumPasswordLength`	Numero minimo di caratteri nella password	Numero intero	Da 8 a 128	8
`PasswordReusePrevention`	Numero di rotazioni della password prima che una vecchia password possa essere riutilizzata	Numero intero	Da 12 a 24	Nessun valore predefinito
`MaxPasswordAge`	Numero di giorni prima della scadenza della password	Numero intero	Da 1 a 90	Nessun valore predefinito

Questo controllo verifica se la politica sulle password degli account per gli utenti IAM utilizza configurazioni complesse. Il controllo fallisce se la politica delle password non utilizza configurazioni complesse. A meno che non si forniscano valori di parametro personalizzati, Security Hub CSPM utilizza i valori predefiniti menzionati nella tabella precedente. I `MaxPasswordAge` parametri `PasswordReusePrevention` and non hanno un valore predefinito, quindi se si escludono questi parametri, Security Hub CSPM ignora il numero di rotazioni della password e l'età della password durante la valutazione di questo controllo.

Per accedere a, gli utenti IAM necessitano di Console di gestione AWS password. Come best practice, Security Hub CSPM consiglia vivamente di utilizzare la federazione anziché creare utenti IAM. La federazione consente agli utenti di utilizzare le credenziali aziendali esistenti per accedere a. Console di gestione AWS Utilizza Centro identità AWS IAM (IAM Identity Center) per creare o federare l'utente, quindi assumi un ruolo IAM in un account.

Per ulteriori informazioni sui provider di identità e sulla federazione, consulta Provider di identità e federazione nella Guida per l'utente IAM. Per ulteriori informazioni su IAM Identity Center, consulta la Guida Centro identità AWS IAM per l'utente.

Se è necessario utilizzare utenti IAM, Security Hub CSPM consiglia di imporre la creazione di password utente complesse. È possibile impostare una politica in materia di password Account AWS per specificare i requisiti di complessità e i periodi di rotazione obbligatori per le password. Quando si crea o si modifica una politica in materia di password, la maggior parte delle impostazioni relative alle password viene applicata alla successiva modifica delle password da parte degli utenti. Alcune impostazioni vengono applicate immediatamente.

Correzione

Per aggiornare la politica sulle password, consulta Impostazione di una politica di password dell'account per gli utenti IAM nella Guida per l'utente IAM.

[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/1.3 NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), (3), NIST.800-53.r5 AC-2 (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 (7), NIST.800-171.r2 3.1.2, PCI NIST.800-53.r5 AC-6 DSS versione 3.2. 1/8.1.4, PCI DSS versione 4.0. 1/8.2.6, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-05.03

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::IAM::User`

Regola AWS Config : `iam-user-unused-credentials-check`

Tipo di pianificazione: periodica

Parametri:

- `maxCredentialUsageAge`: `90` (non personalizzabile)

Questo controllo verifica se gli utenti IAM dispongono di password o chiavi di accesso attive che non vengono utilizzate da 90 giorni.

Gli utenti IAM possono accedere alle AWS risorse utilizzando diversi tipi di credenziali, come password o chiavi di accesso.

Security Hub CSPM consiglia di rimuovere o disattivare tutte le credenziali inutilizzate per 90 giorni o più. La disabilitazione o la rimozione di credenziali non necessarie riduce la finestra di opportunità per le credenziali associate a un account compromesso o abbandonato da utilizzare.

> **Note**
>
> AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub CSPM. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Quando visualizzi le informazioni sull'utente nella console IAM, ci sono colonne relative all'età della chiave di accesso, all'età della password e all'ultima attività. Se il valore in una di queste colonne è maggiore di 90 giorni, rendi inattive le credenziali per tali utenti.

Puoi anche utilizzare i report sulle credenziali per monitorare gli utenti e identificare quelli che non svolgono alcuna attività per 90 o più giorni. Puoi scaricare i report sulle credenziali in `.csv` formato dalla console IAM.

Dopo aver identificato gli account inattivi o le credenziali non utilizzate, disattivali. Per istruzioni, consulta Creazione, modifica o eliminazione di una password utente IAM (console) nella Guida per l'utente IAM.

[IAM.9] L'MFA deve essere abilitata per l'utente root

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.4, PCI DSS v3.2. 1/8.3.1, PCI DSS versione 4.0. 1/8.4.2, benchmark AWS CIS Foundations v3.0. 0/1.5, benchmark AWS CIS Foundations v1.4. 0/1.5, benchmark AWS CIS Foundations v1.2. 0/1.13, 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), Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-05.02

Categoria: Protezione > Gestione degli accessi sicuri

Severità: critica

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `root-account-mfa-enabled`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se l'autenticazione a più fattori (MFA) è abilitata per l'utente root IAM di Account AWS un utente che accede a. Console di gestione AWS Il controllo fallisce se l'MFA non è abilitata per l'utente root dell'account.

L'utente root IAM di an Account AWS ha accesso completo a tutti i servizi e le risorse dell'account. Se l'MFA è abilitata, l'utente deve inserire un nome utente, una password e un codice di autenticazione dal proprio dispositivo AWS MFA per accedere a. Console di gestione AWS L'MFA aggiunge un ulteriore livello di protezione oltre a nome utente e password.

Questo controllo genera `PASSED` risultati nei seguenti casi:

- Le credenziali dell'utente root sono presenti nell'account e l'MFA è abilitata per l'utente root.
- Le credenziali dell'utente root non sono presenti nell'account.

Il controllo genera `FAILED` risultati se le credenziali dell'utente root sono presenti nell'account e l'MFA non è abilitata per l'utente root.

Correzione

Per informazioni sull'attivazione della MFA per l'utente root di un Account AWS, consulta la sezione relativa all'Multi-factor autenticazione Utente root dell'account AWS nella Guida per l'AWS Identity and Access Management utente.

[IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide

Requisiti correlati: NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, 3.5.8, PCI DSS NIST.800-171.r2 v3.2. 1/8.1.4, PCI DSS versione 3.2. 1/8.2.3, PCI DSS versione 3.2. 1/8.2.4, PCI DSS versione 3.2. 1/8.2.5, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-05.02

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `iam-password-policy`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la politica delle password degli account per gli utenti IAM utilizza le seguenti configurazioni PCI DSS minime.

- `RequireUppercaseCharacters`— Richiede almeno un carattere maiuscolo nella password. L'impostazione predefinita è `true`.
- `RequireLowercaseCharacters`— Richiede almeno un carattere minuscolo nella password. L'impostazione predefinita è `true`.
- `RequireNumbers`— Richiedi almeno un numero nella password. L'impostazione predefinita è `true`.
- `MinimumPasswordLength`— Lunghezza minima della password. (Impostazione predefinita = 7 o più)
- `PasswordReusePrevention`— Numero di password prima di consentirne il riutilizzo. (Impostazione predefinita = 4)
- `MaxPasswordAge`— Numero di giorni prima della scadenza della password. (Impostazione predefinita = 90)

> **Note**
>
> Il 30 maggio 2025, Security Hub CSPM ha rimosso questo controllo dallo standard PCI DSS v4.0.1. PCI DSS v4.0.1 ora richiede che le password abbiano un minimo di 8 caratteri. Questo controllo continua ad applicarsi allo standard PCI DSS v3.2.1, che ha requisiti di password diversi.
> Per valutare le politiche relative alle password degli account rispetto ai requisiti PCI DSS v4.0.1, puoi utilizzare il controllo. IAM.7 Questo controllo richiede che le password abbiano un minimo di 8 caratteri. Supporta anche valori personalizzati per la lunghezza della password e altri parametri. Il IAM.7 controllo fa parte dello standard PCI DSS v4.0.1 in Security Hub CSPM.

Correzione

Per aggiornare la politica sulle password per utilizzare la configurazione consigliata, consulta Impostazione di una politica di password dell'account per gli utenti IAM nella Guida per l'utente IAM.

[IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/1.5, NIST.800-171.r2 3.5.7, PCI DSS versione 4.0. 1/83.3.6, PCI DSS versione 4.0. 1/8.6.3, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-03.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `iam-password-policy`

Tipo di pianificazione: periodica

Parametri: nessuno

Le policy sulle password applicano, in parte, requisiti di conformità delle password. Utilizza le politiche di gestione delle password di IAM per assicurarti che le password utilizzino set di caratteri diversi.

Il CIS raccomanda che la politica delle password richieda almeno una lettera maiuscola. L'impostazione di una policy di complessità delle password aumenta la resilienza dell'account a fronte di tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta Impostazione di una politica di password dell'account per gli utenti IAM nella Guida per l'utente IAM. Per la sicurezza della password, seleziona Richiedi almeno una lettera maiuscola dell'alfabeto latino (A—Z).

[IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/1.6, NIST.800-171.r2 3.5.7, PCI DSS versione 4.0. 1/83.3.6, PCI DSS versione 4.0. 1/8.6.3, Profilo CRI v2. 2/PR. AA-01.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `iam-password-policy`

Tipo di pianificazione: periodica

Parametri: nessuno

Le policy sulle password applicano, in parte, requisiti di conformità delle password. Utilizza le politiche di gestione delle password di IAM per assicurarti che le password utilizzino set di caratteri diversi. Il CIS consiglia che la politica delle password richieda almeno una lettera minuscola. L'impostazione di una policy di complessità delle password aumenta la resilienza dell'account a fronte di tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta Impostazione di una politica di password dell'account per gli utenti IAM nella Guida per l'utente IAM. Per la sicurezza della password, seleziona Richiedi almeno una lettera minuscola dell'alfabeto latino (A—Z).

[IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/1.7, NIST.800-171.r2 3.5.7, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-03.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `iam-password-policy`

Tipo di pianificazione: periodica

Parametri: nessuno

Le policy sulle password applicano, in parte, requisiti di conformità delle password. Utilizza le politiche di gestione delle password di IAM per assicurarti che le password utilizzino set di caratteri diversi.

Il CIS raccomanda che la politica delle password richieda almeno un simbolo. L'impostazione di una policy di complessità delle password aumenta la resilienza dell'account a fronte di tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta Impostazione di una politica di password dell'account per gli utenti IAM nella Guida per l'utente IAM. Per la sicurezza della password, seleziona Richiedi almeno un carattere non alfanumerico.

[IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/1.8, NIST.800-171.r2 3.5.7, PCI DSS versione 4.0. 1/83.3.6, PCI DSS versione 4.0. 1/8.6.3, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-03.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `iam-password-policy`

Tipo di pianificazione: periodica

Parametri: nessuno

Le policy sulle password applicano, in parte, requisiti di conformità delle password. Utilizza le politiche di gestione delle password di IAM per assicurarti che le password utilizzino set di caratteri diversi.

Il CIS raccomanda che la politica delle password richieda almeno un numero. L'impostazione di una policy di complessità delle password aumenta la resilienza dell'account a fronte di tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta Impostazione di una politica di password dell'account per gli utenti IAM nella Guida per l'utente IAM. Per la sicurezza della password, seleziona Richiedi almeno un numero.

[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.7, benchmark AWS CIS Foundations v3.0. 0/1.8, benchmark AWS CIS Foundations v1.4. 0/1.8, benchmark AWS CIS Foundations v1.2. 0/1.9, NIST.800-171.r2 3.5.7, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-03.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `iam-password-policy`

Tipo di pianificazione: periodica

Parametri: nessuno

Le policy sulle password applicano, in parte, requisiti di conformità delle password. Utilizza le politiche di gestione delle password di IAM per assicurarti che le password abbiano almeno una determinata lunghezza.

Il CIS raccomanda che la politica delle password richieda una lunghezza minima della password di 14 caratteri. L'impostazione di una policy di complessità delle password aumenta la resilienza dell'account a fronte di tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta Impostazione di una politica di password dell'account per gli utenti IAM nella Guida per l'utente IAM. Per la lunghezza minima della password, inserisci **14** o un numero maggiore.

[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.8, benchmark AWS CIS Foundations v3.0. 0/1.9, benchmark AWS CIS Foundations v1.4. 0/1.9, benchmark AWS CIS Foundations v1.2. 0/1.10, NIST.800-171.r2 3.5.8, PCI DSS versione 4.0. 1/8.3.7, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-03.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `iam-password-policy`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se il numero di password da ricordare è impostato su 24. Il controllo ha esito negativo se il valore non è 24.

Le policy di gestione delle password di IAM possono impedire il riutilizzo di una determinata password da parte dello stesso utente.

Il CIS raccomanda che la politica sulle password impedisca il riutilizzo delle password. Impedire il riutilizzo delle password consente di incrementare la resilienza dell'account rispetto a tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta Impostazione di una politica di password dell'account per gli utenti IAM nella Guida per l'utente IAM. Per Impedire il riutilizzo della password, inserisci**24**.

[IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/1.11, PCI DSS versione 4.0. 1/8.3.9, PCI DSS versione 4.0. 1/8.3.10.1, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-03.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `iam-password-policy`

Tipo di pianificazione: periodica

Parametri: nessuno

Le politiche relative alle password di IAM possono richiedere la rotazione o la scadenza delle password dopo un determinato numero di giorni.

Il CIS consiglia che la politica sulle password faccia scadere le password dopo 90 giorni o meno. La riduzione della durata della password aumenta la resilienza dell'account contro tentativi di accesso di forza bruta. Richiedere le modifiche regolari delle password è utile nelle seguenti situazioni:

- Le password possono essere rubate o compromesse senza saperlo. Questo può accadere tramite compromissione del sistema, vulnerabilità del software o minacce interne.
- Alcuni filtri Web aziendali e governativi o server proxy sono in grado di intercettare e registrare il traffico anche se è criptato.
- Molte persone utilizzano la stessa password per molti sistemi diversi come lavoro, e-mail e personale.
- Workstation dell'utente finale compromesse potrebbero includere un keystroke logger.

Correzione

Per modificare la politica relativa alle password, consulta Impostazione di una politica di password dell'account per gli utenti IAM nella Guida per l'utente IAM. Per attivare la scadenza della password, inserisci **`90`** o un numero inferiore.

[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.16, benchmark AWS CIS Foundations v3.0. 0/1.17, benchmark AWS CIS Foundations v1.4. 0/1.17, benchmark AWS CIS Foundations v1.2.

0/1.20, NIST.800-171.r2 3.1.2, PCI DSS versione 4.0. 1/12.10.3, Profilo CRI v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-04.01, Profilo CRI v2. 2/PR. AA-05.02

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `iam-policy-in-use`

Tipo di pianificazione: periodica

Parametri:

- `policyARN`: `arn:partition:iam::aws:policy/AWSSupportAccess` (non personalizzabile)
- `policyUsageType`: `ANY` (non personalizzabile)

AWS fornisce un centro di supporto che può essere utilizzato per la notifica e la risposta agli incidenti, nonché per il supporto tecnico e il servizio clienti.

Crea un ruolo IAM per consentire agli utenti autorizzati di gestire gli incidenti con AWS Support. Implementando il privilegio minimo per il controllo degli accessi, un ruolo IAM richiederà una policy IAM appropriata per consentire l'accesso al centro di supporto per gestire gli incidenti con. Supporto

> **Note**
>
> AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub CSPM. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per risolvere questo problema, crea un ruolo che consenta agli utenti autorizzati di gestire gli Supporto incidenti.

Per creare il ruolo da utilizzare per Supporto accedi

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.

2. Nel riquadro di navigazione IAM, scegli Ruoli, quindi scegli Crea ruolo.
3. Per Tipo di ruolo, scegli Altro Account AWS.
4. Per ID account, inserisci l' Account AWS ID Account AWS a cui desideri concedere l'accesso alle tue risorse.

   Se gli utenti o i gruppi che assumeranno questo ruolo si trovano nello stesso account, immettere il numero di account locale.

   > **Note**
   >
   > L'amministratore dell'account specificato può concedere l'autorizzazione di assumere questo ruolo a qualsiasi utente in tale account. Per eseguire questa operazione, l'amministratore collega una policy all'utente o al gruppo che garantisce l'autorizzazione per l'operazione `sts:AssumeRole`. In tale policy, la risorsa deve essere l'ARN del ruolo.

5. Scegli Successivo: autorizzazioni.
6. Cercare la policy gestita `AWSSupportAccess`.
7. Selezionare la casella di controllo per la policy gestita `AWSSupportAccess`.
8. Scegli Successivo: Tag.
9. (Facoltativo) Per aggiungere metadati al ruolo, allega i tag come coppie chiave-valore.

   Per ulteriori informazioni sull'utilizzo dei tag in IAM, vedere Tagging di utenti e ruoli IAM nella Guida per l'utente di IAM.
10. Scegli Prossimo: Rivedi.
11. In Nome ruolo, immetti un nome per il ruolo.

    I nomi dei ruoli devono essere univoci all'interno del tuo. Account AWS Non rispettano la distinzione tra maiuscole e minuscole.
12. (Facoltativo) In Descrizione ruolo, immettere una descrizione per il nuovo ruolo.
13. Verificare il ruolo e scegliere Create role (Crea ruolo).

[IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM

Requisiti correlati: 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 (8), NIST.800-53.r5 IA-2 3.3.8, NIST.800-171.r2 3.5.3,

NIST.800-171.r2 NIST.800-171.r2 3.5.4, 3.7.5, PCI DSS v3.2. NIST.800-171.r2 1/83.3.1, PCI DSS versione 4.0. 1/8.4.2, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-05.02

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::IAM::User`

Regola AWS Config : `iam-user-mfa-enabled`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se gli utenti IAM hanno abilitato l'autenticazione a più fattori (MFA).

> **Note**
>
> AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub CSPM. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per aggiungere MFA per gli utenti IAM, consulta Enabling MFA devices for users AWS nella IAM User Guide.

[IAM.20] Evita l'uso dell'utente root

> **Important**
>
> Security Hub CSPM ha ritirato questo controllo nell'aprile 2024. Per ulteriori informazioni, consulta Registro delle modifiche per i controlli CSPM di Security Hub.

Requisiti correlati: CIS AWS Foundations Benchmark v1.2. 0/11.

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: `AWS::IAM::User`

AWS Config regola: `use-of-root-account-test` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un Account AWS ha restrizioni sull'utilizzo dell'utente root. Il controllo valuta le seguenti risorse:

- Argomenti su Amazon Simple Notification Service (Amazon SNS)
- AWS CloudTrail sentieri
- Filtri metrici associati ai sentieri CloudTrail
- CloudWatch Allarmi Amazon basati sui filtri

Questo controllo determina se `FAILED` una o più delle seguenti affermazioni sono vere:

- Non esistono CloudTrail percorsi nell'account.
- Un CloudTrail percorso è abilitato, ma non configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura.
- Un CloudTrail trail è abilitato, ma non è associato a un gruppo di CloudWatch log Logs.
- Il filtro metrico esatto prescritto dal Center for Internet Security (CIS) non viene utilizzato. Il filtro metrico prescritto è. `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`
- Nell' CloudWatch account non sono presenti allarmi basati sul filtro metrico.
- CloudWatch gli allarmi configurati per inviare notifiche all'argomento SNS associato non si attivano in base alla condizione di allarme.
- L'argomento SNS non è conforme ai vincoli per l'invio di un messaggio a un argomento SNS.
- L'argomento SNS non ha almeno un sottoscrittore.

Questo controllo determina `NO_DATA` se una o più delle seguenti affermazioni sono vere:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub CSPM può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub CSPM può generare risultati solo per l'account proprietario del percorso.

Questo controllo determina `WARNING` se una o più delle seguenti affermazioni sono vere:

- L'account corrente non possiede l'argomento SNS a cui si fa riferimento nell' CloudWatch avviso.
- L'account corrente non ha accesso all'argomento SNS quando richiama l'API SNS. `ListSubscriptionsByTopic`

> **Note**
>
> Ti consigliamo di utilizzare gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta lo stato di controllo NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub CSPM genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato CSPM di Security Hub utilizzando l'aggregazione tra regioni.

Come best practice, utilizzare le credenziali dell'utente root solo quando necessario per eseguire attività di gestione degli account e dei servizi. Applica le policy IAM direttamente ai gruppi e ai ruoli, ma non agli utenti. Per istruzioni sulla configurazione di un amministratore per l'uso quotidiano, consulta Creazione del primo utente e gruppo di amministratori IAM nella Guida per l'utente IAM.

Correzione

I passaggi per risolvere questo problema includono la configurazione di un argomento di Amazon SNS, CloudTrail un percorso, un filtro metrico e un allarme per il filtro metrico.

Come creare un argomento Amazon SNS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.

2. Crea un argomento Amazon SNS che riceva tutti gli allarmi CIS.

   Creare almeno un sottoscrittore all'argomento. Per ulteriori informazioni, consulta Nozioni di base su Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Quindi, configura un attivo CloudTrail che si applichi a tutte le regioni. A questo scopo, seguire le fasi di correzione in the section called "[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura".

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Crei il filtro metrico per quel gruppo di log.

Infine, crea il filtro metrico e l'allarme.

Per creare un filtro parametri e allarme

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, selezionare Log groups (Gruppi di log).
3. Seleziona la casella di controllo per il gruppo di log CloudWatch Logs associato al CloudTrail percorso che hai creato.
4. Da Azioni, scegli Crea filtro metrico.
5. In Definisci modello, procedi come segue:

   a. Copiare il seguente modello e incollarlo nel campo Filter Pattern (Modello di filtro).

   ```
   {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
    $.eventType !="AwsServiceEvent"}
   ```

   b. Scegli Avanti.
6. In Assegna metrica, effettuate le seguenti operazioni:

   a. In Nome filtro, inserisci un nome per il filtro metrico.

   b. Per Metric Namespace, inserisci. **`LogMetrics`**

      Se si utilizza lo stesso spazio dei nomi per tutti i filtri delle metriche dei log CIS, tutte le metriche di CIS Benchmark vengono raggruppate insieme.

   c. Per Metric Name, inserisci un nome per la metrica. Ricorda il nome della metrica. Dovrai selezionare la metrica quando crei l'allarme.

d. In Metric value (Valore parametro), inserisci **1**.

e. Scegli Avanti.

7. In Rivedi e crea, verifica le informazioni che hai fornito per il nuovo filtro metrico. Quindi, scegli Crea filtro metrico.
8. Nel riquadro di navigazione, scegli Gruppi di log, quindi scegli il filtro che hai creato in Filtri metrici.
9. Seleziona la casella di controllo per il filtro. Scegli Crea allarme.
10. In Specificare metriche e condizioni, procedi come segue:

    a. In Condizioni, per Soglia, scegli Statico.

    b. Per Definire la condizione di allarme, scegli Greater/Equal.

    c. Per Definire il valore di soglia, immettere**1**.

    d. Scegli Avanti.

11. In Configura azioni, procedi come segue:

    a. In Attivazione dello stato di allarme, scegli In allarme.

    b. In Select an SNS topic (Seleziona un argomento SNS), scegli Select an existing SNS topic (Seleziona un argomento SNS esistente).

    c. In Invia una notifica a, inserisci il nome dell'argomento SNS creato nella procedura precedente.

    d. Scegli Avanti.

12. In Aggiungi nome e descrizione, inserisci un nome e una descrizione per l'avviso, ad esempio**`CIS-1.1-RootAccountUsage`**. Quindi scegli Successivo.
13. In Anteprima e crea, rivedi la configurazione dell'allarme. Quindi scegli Crea allarme.

[IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi

Requisiti correlati: 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), (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, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Rileva > Gestione sicura degli accessi

Gravità: bassa

Tipo di risorsa: `AWS::IAM::Policy`

Regola AWS Config : `iam-policy-no-statements-with-full-access`

Tipo di pianificazione: modifica attivata

Parametri:

- `excludePermissionBoundaryPolicy`: `True` (non personalizzabile)

Questo controllo verifica se le policy basate sull'identità IAM che crei dispongono di istruzioni Allow che utilizzano la wildcard * per concedere le autorizzazioni per tutte le azioni su qualsiasi servizio. Il controllo ha esito negativo se una dichiarazione di policy include with. `"Effect": "Allow"` `"Action": "Service:*"`

Ad esempio, la seguente dichiarazione in una politica comporta un errore di ricerca.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

Il controllo ha esito negativo anche se si utilizza `"Effect": "Allow"` con`"NotAction": "service:*"`. In tal caso, l'`NotAction`elemento fornisce l'accesso a tutte le azioni di un Servizio AWS, ad eccezione delle azioni specificate in`NotAction`.

Questo controllo si applica solo alle politiche IAM gestite dal cliente. Non si applica alle policy IAM gestite da AWS.

Quando si assegnano le autorizzazioni a Servizi AWS, è importante definire l'ambito delle azioni IAM consentite nelle politiche IAM. È necessario limitare le azioni IAM solo alle azioni necessarie. Questo ti aiuta a fornire i permessi con privilegi minimi. Politiche eccessivamente permissive potrebbero portare a un aumento dei privilegi se le policy sono collegate a un principale IAM che potrebbe non richiedere l'autorizzazione.

In alcuni casi, potresti voler consentire azioni IAM con un prefisso simile, come e. `DescribeFlowLogs` `DescribeAvailabilityZones` In questi casi autorizzati, puoi aggiungere un carattere jolly con suffisso al prefisso comune. Ad esempio, `ec2:Describe*`.

Questo controllo passa se si utilizza un'azione IAM con prefisso e un carattere jolly con suffisso. Ad esempio, la seguente dichiarazione in una politica restituisce un risultato positivo.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

Raggruppando le azioni IAM correlate in questo modo, puoi anche evitare di superare i limiti di dimensione delle policy IAM.

> **Note**
>
> AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub CSPM. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per risolvere questo problema, aggiorna le policy IAM in modo che non consentano i privilegi amministrativi «*» completi. Per i dettagli su come modificare una policy IAM, consulta Modifica delle policy IAM nella IAM User Guide.

[IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.11, benchmark AWS CIS Foundations v3.0. 0/1.12, benchmark AWS CIS Foundations v1.4. 0/1.12, NIST.800-171.r2 3.1.2, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-05.03

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::IAM::User`

AWS Config regola: **`iam-user-unused-credentials-check`**

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se gli utenti IAM dispongono di password o chiavi di accesso attive che non vengono utilizzate da 45 giorni o più. A tal fine, verifica se il `maxCredentialUsageAge` parametro della AWS Config regola è uguale o superiore a 45.

Gli utenti possono accedere alle AWS risorse utilizzando diversi tipi di credenziali, come password o chiavi di accesso.

Il CIS consiglia di rimuovere o disattivare tutte le credenziali che non sono state utilizzate per 45 giorni o più. La disabilitazione o la rimozione di credenziali non necessarie riduce la finestra di opportunità per le credenziali associate a un account compromesso o abbandonato da utilizzare.

La AWS Config regola per questo controllo utilizza le operazioni `GetCredentialReport`e `GenerateCredentialReport`API, che vengono aggiornate solo ogni quattro ore. Le modifiche agli utenti IAM possono richiedere fino a quattro ore per essere visibili a questo controllo.

> **Note**
>
> AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub CSPM. Tuttavia, è possibile abilitare la registrazione delle risorse globali in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Quando visualizzi le informazioni sull'utente nella console IAM, ci sono colonne relative all'età della chiave di accesso, all'età della password e all'ultima attività. Se il valore in una di queste colonne è superiore a 45 giorni, rendi inattive le credenziali di tali utenti.

Puoi anche utilizzare i report sulle credenziali per monitorare gli utenti e identificare quelli che non svolgono alcuna attività per 45 o più giorni. Puoi scaricare i report sulle credenziali in `.csv` formato dalla console IAM.

Dopo aver identificato gli account inattivi o le credenziali non utilizzate, disattivali. Per istruzioni, consulta Creazione, modifica o eliminazione di una password utente IAM (console) nella Guida per l'utente IAM.

[IAM.23] Gli analizzatori IAM Access Analyzer devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::AccessAnalyzer::Analyzer`

AWS Config regola: `tagged-accessanalyzer-analyzer` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un analizzatore gestito da AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'analizzatore non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'analizzatore non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un analizzatore, consulta TagResourceAWSIAM Access Analyzer API Reference.

[IAM.24] I ruoli IAM devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IAM::Role`

AWS Config regola: `tagged-iam-role` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un ruolo AWS Identity and Access Management (IAM) ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il ruolo non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il ruolo non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un ruolo IAM, consulta Tagging IAM resources nella IAM User Guide.

[IAM.25] Gli utenti IAM devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IAM::User`

AWS Config regola: `tagged-iam-user` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un utente AWS Identity and Access Management (IAM) dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'utente non dispone di alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'utente non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un utente IAM, consulta Tagging IAM resources nella IAM User Guide.

[IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.18, benchmark AWS CIS Foundations v3.0. 0/1.19, Profilo CRI v2. 2/PR. PS-01.07

Categoria: Identificazione > Conformità

Gravità: media

Tipo di risorsa: `AWS::IAM::ServerCertificate`

AWS Config regola: **`iam-server-certificate-expiration-check`**

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un certificato di SSL/TLS server attivo gestito in IAM è scaduto. Il controllo fallisce se il certificato del SSL/TLS server scaduto non viene rimosso.

Per abilitare le connessioni HTTPS al sito Web o all'applicazione in AWS, è necessario un certificato SSL/TLS server. Puoi utilizzare IAM o AWS Certificate Manager (ACM) per archiviare e distribuire i certificati del server. Utilizza IAM come gestore di certificati solo quando devi supportare connessioni HTTPS in un ambiente Regione AWS non supportato da ACM. IAM crittografa in modo sicuro le chiavi private e archivia la versione crittografata nella memoria dei certificati SSL di IAM. IAM supporta la distribuzione di certificati server in tutte le regioni, ma è necessario ottenere il certificato da un provider esterno per utilizzarlo con. AWS Non puoi caricare un certificato ACM su IAM. Inoltre, non puoi gestire i tuoi certificati dalla console IAM. La rimozione SSL/TLS dei certificati scaduti elimina il rischio che un certificato non valido venga distribuito accidentalmente su una risorsa, il che può danneggiare la credibilità dell'applicazione o del sito Web sottostante.

Correzione

Per rimuovere un certificato server da IAM, consulta Managing server certificates in IAM nella IAM User Guide.

[IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.21, benchmark AWS CIS Foundations v3.0. 0/1.22, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Gestione sicura degli accessi > Policy IAM sicure

Gravità: media

Tipo di risorsa:`AWS::IAM::Role`,`AWS::IAM::User`, `AWS::IAM::Group`

AWS Config regola: **`iam-policy-blacklisted-check`**

Tipo di pianificazione: modifica attivata

Parametri:

- «Policyarns»: «arn:aws:iam: :aws:, arn:aws-cn:iam: :aws:, arn:aws-us-gov:iampolicy/AWSCloudShellFullAccess: :aws:» policy/AWSCloudShellFullAccess policy/AWSCloudShellFullAccess

Questo controllo verifica se a un'identità IAM (utente, ruolo o gruppo) è associata la policy gestita AWS . `AWSCloudShellFullAccess` Il controllo fallisce se a un'identità IAM è associata la `AWSCloudShellFullAccess` policy.

AWS CloudShell fornisce un modo conveniente per eseguire comandi CLI. Servizi AWS La policy AWS gestita `AWSCloudShellFullAccess` fornisce l'accesso completo a CloudShell, che consente la funzionalità di caricamento e download di file tra il sistema locale dell'utente e l' CloudShell ambiente. All'interno dell' CloudShell ambiente, un utente dispone delle autorizzazioni sudo e può accedere a Internet. Di conseguenza, l'associazione di questa policy gestita a un'identità IAM offre loro la possibilità di installare software per il trasferimento di file e spostare i dati CloudShell da server Internet esterni. Ti consigliamo di seguire il principio del privilegio minimo e di assegnare autorizzazioni più limitate alle tue identità IAM.

Correzione

Per scollegare la *`AWSCloudShellFullAccess`* policy da un'identità IAM, consulta Aggiungere e rimuovere le autorizzazioni di identità IAM nella Guida per l'utente IAM.

[IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/1.19, benchmark AWS CIS Foundations v3.0. 0/1.20, Profilo CRI v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. AA-05.04

Categoria: Rileva > Servizi di rilevamento > Monitoraggio dell'utilizzo privilegiato

Gravità: alta

Tipo di risorsa: `AWS::AccessAnalyzer::Analyzer`

AWS Config regola: **`iam-external-access-analyzer-enabled`**

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un Account AWS ha un analizzatore di accesso esterno IAM Access Analyzer abilitato. Il controllo fallisce se l'account non ha un analizzatore di accesso esterno abilitato nell'area attualmente selezionata. Regione AWS

Gli analizzatori di accesso esterni IAM Access Analyzer aiutano a identificare le risorse, come i bucket Amazon Simple Storage Service (Amazon S3) o i ruoli IAM, che sono condivisi con un'entità esterna. Questo ti aiuta a evitare l'accesso involontario alle tue risorse e ai tuoi dati. IAM Access Analyzer è regionale e deve essere abilitato in ogni regione. Per identificare le risorse condivise con responsabili esterni, un analizzatore di accessi utilizza il ragionamento basato sulla logica per

analizzare le politiche basate sulle risorse nel tuo ambiente. AWS Quando si crea un analizzatore di accessi esterno, è possibile crearlo e attivarlo per l'intera organizzazione o per singoli account.

> **Note**
>
> Se un account fa parte di un'organizzazione in AWS Organizations, questo controllo non tiene conto degli analizzatori di accesso esterni che specificano l'organizzazione come zona di fiducia e sono abilitati per l'organizzazione nella regione corrente. Se l'organizzazione utilizza questo tipo di configurazione, valuta la possibilità di disabilitare questo controllo per gli account dei singoli membri dell'organizzazione nella regione.

Correzione

Per informazioni sull'attivazione di un analizzatore di accesso esterno in una regione specifica, consulta Guida introduttiva a IAM Access Analyzer nella IAM User Guide. È necessario abilitare un analizzatore in ogni regione in cui si desidera monitorare l'accesso alle risorse.

Controlli CSPM di Security Hub per Amazon Inspector

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse di Amazon Inspector.

Questi controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata

Requisiti correlati: PCI DSS v4.0. 1/11.3.1, Profilo CRI v2. 2/ID. RA-01.03, Profilo CRI v2. 2/PR. PS-02.02

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS:::Account`

Regola AWS Config : `inspector-ec2-scan-enabled`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la scansione di Amazon Inspector EC2 è abilitata. Per un account indipendente, il controllo fallisce se la scansione di Amazon Inspector EC2 è disabilitata nell'account. In un ambiente con più account, il controllo fallisce se l'account amministratore delegato di Amazon Inspector o qualsiasi account membro associato non ha abilitato la scansione EC2.

In un ambiente con più account, il controllo genera risultati solo nell'account amministratore delegato di Amazon Inspector. Solo l'amministratore delegato può abilitare o disabilitare la funzionalità di scansione EC2 per gli account dei membri dell'organizzazione. Gli account membri di Amazon Inspector non possono modificare questa configurazione dai loro account. Questo controllo genera `FAILED` risultati se l'amministratore delegato ha un account membro sospeso che non ha la scansione Amazon Inspector EC2 abilitata. Per ricevere un `PASSED` risultato, l'amministratore delegato deve dissociare questi account sospesi in Amazon Inspector.

La scansione di Amazon Inspector EC2 estrae i metadati dalla tua istanza Amazon Elastic Compute Cloud (Amazon EC2), quindi confronta questi metadati con le regole raccolte dagli avvisi di sicurezza per produrre risultati. Amazon Inspector analizza le istanze alla ricerca di vulnerabilità dei pacchetti e problemi di raggiungibilità della rete. Per informazioni sui sistemi operativi supportati, incluso il sistema operativo che può essere scansionato senza un agente SSM, consulta Sistemi operativi supportati: scansione Amazon EC2.

Correzione

Per abilitare la scansione di Amazon Inspector EC2, consulta Attivazione delle scansioni nella Guida per l'utente di Amazon Inspector.

[Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata

Requisiti correlati: PCI DSS v4.0. 1/11.3.1, Profilo CRI v2. 2/ID. RA-01.03, Profilo CRI v2. 2/PR. PS-02.02

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `inspector-ecr-scan-enabled`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la scansione ECR di Amazon Inspector è abilitata. Per un account indipendente, il controllo fallisce se la scansione ECR di Amazon Inspector è disabilitata nell'account. In un ambiente con più account, il controllo fallisce se l'account amministratore delegato di Amazon Inspector o qualsiasi account membro associato non ha abilitato la scansione ECR.

In un ambiente con più account, il controllo genera risultati solo nell'account amministratore delegato di Amazon Inspector. Solo l'amministratore delegato può abilitare o disabilitare la funzionalità di scansione ECR per gli account dei membri dell'organizzazione. Gli account membri di Amazon Inspector non possono modificare questa configurazione dai loro account. Questo controllo genera `FAILED` risultati se l'amministratore delegato ha un account membro sospeso che non ha la scansione ECR di Amazon Inspector abilitata. Per ricevere un `PASSED` risultato, l'amministratore delegato deve dissociare questi account sospesi in Amazon Inspector.

Amazon Inspector analizza le immagini dei container archiviate in Amazon Elastic Container Registry (Amazon ECR) alla ricerca di vulnerabilità del software per generare risultati sulle vulnerabilità dei pacchetti. Quando attivi le scansioni Amazon Inspector per Amazon ECR, imposti Amazon Inspector come servizio di scansione preferito per il tuo registro privato. Questo sostituisce la scansione di base, fornita gratuitamente da Amazon ECR, con la scansione avanzata, fornita e fatturata tramite Amazon Inspector. La scansione avanzata offre il vantaggio della scansione delle vulnerabilità sia per il sistema operativo che per i pacchetti di linguaggi di programmazione a livello di registro. Puoi esaminare i risultati scoperti utilizzando la scansione avanzata a livello di immagine, per ogni livello dell'immagine, sulla console Amazon ECR. Inoltre, puoi esaminare e utilizzare questi risultati in altri servizi non disponibili per le scansioni di base, AWS Security Hub CSPM tra cui Amazon EventBridge.

Correzione

Per abilitare la scansione Amazon Inspector ECR, consulta Attivazione delle scansioni nella Guida per l'utente di Amazon Inspector.

[Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata

Requisiti correlati: PCI DSS v4.0. 1/62.2.4, PCI DSS versione 4.0. 1/6.3.1, Profilo CRI v2. 2/ID. RA-01.03, Profilo CRI v2. 2/PR. PS-02.02

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS:::::Account`

Regola AWS Config : `inspector-lambda-code-scan-enabled`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la scansione del codice Amazon Inspector Lambda è abilitata. Per un account indipendente, il controllo fallisce se la scansione del codice Amazon Inspector Lambda è disabilitata nell'account. In un ambiente con più account, il controllo fallisce se l'account amministratore delegato di Amazon Inspector o qualsiasi account membro associato non ha abilitato la scansione del codice Lambda.

In un ambiente con più account, il controllo genera risultati solo nell'account amministratore delegato di Amazon Inspector. Solo l'amministratore delegato può abilitare o disabilitare la funzionalità di scansione del codice Lambda per gli account dei membri dell'organizzazione. Gli account membri di Amazon Inspector non possono modificare questa configurazione dai loro account. Questo controllo genera `FAILED` risultati se l'amministratore delegato ha un account membro sospeso che non ha abilitato la scansione del codice Amazon Inspector Lambda. Per ricevere un `PASSED` risultato, l'amministratore delegato deve dissociare questi account sospesi in Amazon Inspector.

La scansione del codice Amazon Inspector Lambda analizza il codice dell'applicazione personalizzata all'interno di una AWS Lambda funzione alla ricerca di vulnerabilità del codice in base alle best practice di sicurezza. AWS La scansione del codice Lambda può rilevare difetti di iniezione, fughe di dati, crittografia debole o crittografia mancante nel codice. Questa funzionalità è disponibile solo in alcuni casi specifici. Regioni AWS È possibile attivare la scansione del codice Lambda insieme alla scansione standard Lambda (vedi). [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata

Correzione

Per abilitare la scansione del codice Amazon Inspector Lambda, consulta Attivazione delle scansioni nella Guida per l'utente di Amazon Inspector.

[Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata

Requisiti correlati: PCI DSS v4.0. 1/62.2.4, PCI DSS versione 4.0. 1/6.3.1, Profilo CRI v2. 2/ID. RA-01.03, Profilo CRI v2. 2/PR. PS-02.02

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : `inspector-lambda-standard-scan-enabled`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la scansione standard di Amazon Inspector Lambda è abilitata. Per un account indipendente, il controllo fallisce se la scansione standard di Amazon Inspector Lambda è disabilitata nell'account. In un ambiente con più account, il controllo fallisce se l'account amministratore delegato di Amazon Inspector o qualsiasi account membro associato non ha abilitato la scansione standard Lambda.

In un ambiente con più account, il controllo genera risultati solo nell'account amministratore delegato di Amazon Inspector. Solo l'amministratore delegato può abilitare o disabilitare la funzionalità di scansione standard Lambda per gli account dei membri dell'organizzazione. Gli account membri di Amazon Inspector non possono modificare questa configurazione dai loro account. Questo controllo genera `FAILED` risultati se l'amministratore delegato ha un account membro sospeso che non ha la scansione standard Amazon Inspector Lambda abilitata. Per ricevere un `PASSED` risultato, l'amministratore delegato deve dissociare questi account sospesi in Amazon Inspector.

La scansione standard di Amazon Inspector Lambda identifica le vulnerabilità del software nelle dipendenze dei pacchetti applicativi che aggiungi al codice e ai livelli delle funzioni. AWS Lambda Se Amazon Inspector rileva una vulnerabilità nelle dipendenze del pacchetto applicativo della funzione Lambda, Amazon Inspector fornisce una ricerca dettagliata del tipo. `Package Vulnerability` È possibile attivare la scansione del codice Lambda insieme alla scansione standard Lambda (vedi). [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata

Correzione

Per abilitare la scansione standard di Amazon Inspector Lambda, consulta Attivazione delle scansioni nella Guida per l'utente di Amazon Inspector.

Controlli CSPM Security Hub perAWS IoT

Questi AWS Security Hub CSPM controlli valutano il AWS IoT servizio e le risorse.

Questi controlli potrebbero non essere disponibili tuttiRegioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoT::SecurityProfile`

AWS Configregola: `tagged-iot-securityprofile` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	`No default value`

Questo controllo verifica se un profilo AWS IoT Device Defender di sicurezza ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il profilo di sicurezza non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il profilo di sicurezza non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un profilo di AWS IoT Device Defender sicurezza, consulta Tagging your AWS IoT resources nella Developer Guide. AWS IoT

[IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoT::MitigationAction`

AWS Configregola: `tagged-iot-mitigationaction` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfan	`No default value`

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	I tag fanno distinzione tra maiuscole e minuscole		o i requisiti AWS.	

Questo controllo verifica se un'azione di AWS IoT Core mitigazione ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'azione di mitigazione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'azione di mitigazione non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'azione di AWS IoT Core mitigazione, consulta Tagging your AWS IoT resources nella Developer Guide. AWS IoT

[IoT.3]AWS IoT Corele dimensioni devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoT::Dimension`

AWS Configregola: `tagged-iot-dimension` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	`No default value`

Questo controllo verifica se una AWS IoT Core dimensione ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la dimensione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la dimensione non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una

singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una AWS IoT Core dimensione, consulta Tagging your AWS IoT resources nella Developer Guide. AWS IoT

[IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoT::Authorizer`

AWS Configregola: `tagged-iot-authorizer` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	`No default value`

Questo controllo verifica se un AWS IoT Core autorizzatore dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'autorizzatore non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'autorizzatore non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un programma di AWS IoT Core autorizzazione, consulta Tagging your AWS IoT resources nella Developer Guide. AWS IoT

[IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoT::RoleAlias`

AWS Configregola: `tagged-iot-rolealias` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	`No default value`

Questo controllo verifica se un alias di AWS IoT Core ruolo ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo ha esito negativo se l'alias del ruolo non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'alias del ruolo non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un alias di AWS IoT Core ruolo, consulta Tagging your AWS IoT resources nella Developer Guide. AWS IoT

[IoT.6]AWS IoT Corele politiche devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoT::Policy`

AWS Configregola: `tagged-iot-policy` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	`No default value`

Questo controllo verifica se una AWS IoT Core policy ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la policy non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la policy non

è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una AWS IoT Core politica, consulta Tagging your AWS IoT resources nella Developer Guide. AWS IoT

Controlli CSPM Security Hub perAWSIoT SiteWise

Questi AWS Security Hub CSPM controlli valutano il SiteWise servizio e le risorse AWS IoT.

Questi controlli potrebbero non essere disponibili tuttiRegioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTSiteWise::AssetModel`

Regola AWS Config: `iotsitewise-asset-model-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un modello di SiteWise asset AWS IoT ha tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se il modello di asset non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il modello di asset non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un modello di SiteWise asset AWS IoT, consulta Tagga AWS IoT SiteWise le tue risorse nella Guida AWS IoT SiteWise per l'utente.

[IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTSiteWise::Dashboard`

Regola AWS Config: `iotsitewise-dashboard-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se una SiteWise dashboard AWS IoT ha tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se la dashboard non ha alcuna chiave

di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la dashboard non è contrassegnata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a una SiteWise dashboard AWS IoT, consulta Tagga AWS IoT SiteWise le tue risorse nella Guida AWS IoT SiteWise per l'utente.

[IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTSiteWise::Gateway`

Regola AWS Config: `iotsitewise-gateway-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un SiteWise gateway AWS IoT dispone di tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se il gateway non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gateway non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un SiteWise gateway AWS IoT, consulta Etichettare le AWS IoT SiteWise risorse nella Guida AWS IoT SiteWise per l'utente.

[IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTSiteWise::Portal`

Regola AWS Config: `iotsitewise-portal-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un SiteWise portale AWS IoT ha tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se il portale non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il portale non

è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un SiteWise portale AWS IoT, consulta Etichettare le AWS IoT SiteWise risorse nella Guida AWS IoT SiteWise per l'utente.

[IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTSiteWise::Project`

Regola AWS Config: `iotsitewise-project-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un SiteWise progetto AWS IoT ha tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se il progetto non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il progetto non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un SiteWise progetto AWS IoT, consulta Etichettare le AWS IoT SiteWise risorse nella Guida AWS IoT SiteWise per l'utente.

Controlli CSPM Security Hub per AWS IoT TwinMaker

Questi AWS Security Hub CSPM controlli valutano il TwinMaker servizio e le risorse AWS IoT.

Questi controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTTwinMaker::SyncJob`

Regola AWS Config : `iottwinmaker-sync-job-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un processo di TwinMaker sincronizzazione AWS IoT ha tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se il processo

di sincronizzazione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il processo di sincronizzazione non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un processo di TwinMaker sincronizzazione AWS IoT, TagResourceconsulta la Guida AWS IoT TwinMaker per l'utente.

[IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati

Requisiti correlati: CRI Profile v2. 2/ID. AM-01.01, Profilo CRI v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTTwinMaker::Workspace`

Regola AWS Config : `iottwinmaker-workspace-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un' TwinMaker area di lavoro AWS IoT dispone di tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se l'area di lavoro non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredKeyTags` Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'area di lavoro non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un' TwinMaker area di lavoro AWS IoT, consulta TagResourcela Guida per l'AWS IoT TwinMaker utente.

[IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTTwinMaker::Scene`

Regola AWS Config : `iottwinmaker-scene-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se una TwinMaker scena AWS IoT ha tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se la scena non ha alcuna chiave

di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la scena non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a una TwinMaker scena AWS IoT, TagResourceconsulta la Guida AWS IoT TwinMaker per l'utente.

[IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTTwinMaker::Entity`

Regola AWS Config : `iottwinmaker-entity-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un' TwinMaker entità AWS IoT dispone di tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se l'entità non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'entità non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un' TwinMaker entità AWS IoT, TagResourceconsulta la Guida AWS IoT TwinMaker per l'utente.

Controlli CSPM Security Hub perAWSIoT Wireless

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse AWS IoT Wireless.

Questi controlli potrebbero non essere disponibili tuttiRegioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTWireless::MulticastGroup`

Regola AWS Config: `iotwireless-multicast-group-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un gruppo multicast AWS IoT Wireless dispone di tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo ha esito negativo se il gruppo multicast non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredKeyTags` Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo multicast non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un gruppo multicast AWS IoT Wireless, consulta Tagging your Wireless AWS IoT resources nella Wireless AWS IoTDeveloper Guide.

[IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTWireless::ServiceProfile`

Regola AWS Config: `iotwireless-service-profile-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un profilo di servizio AWS IoT Wireless ha tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se il profilo di servizio non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il profilo del servizio non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un profilo di servizio AWS IoT Wireless, consulta Tagging your Wireless AWS IoT resources nella Wireless AWS IoTDeveloper Guide.

[IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoTWireless::FuotaTask`

Regola AWS Config: `iotwireless-fuota-task-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un'attività di aggiornamento del firmware AWS IoT Wireless over-the-air (FUOTA) ha tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo

fallisce se l'attività FUOTA non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredKeyTags` Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'attività FUOTA non è contrassegnata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un'attività FUOTA AWS IoT Wireless, consulta Tagging your Wireless AWS IoT resources nella Wireless AWS IoTDeveloper Guide.

Controlli CSPM del Security Hub per Amazon IVS

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse di Amazon Interactive Video Service (IVS).

Questi controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IVS::PlaybackKeyPair`

Regola AWS Config : `ivs-playback-key-pair-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se una coppia di chiavi di riproduzione Amazon IVS ha tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se la coppia di chiavi di riproduzione non ha alcuna chiave tag o se non ha tutti i tasti specificati nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se la coppia di chiavi di riproduzione non è etichettata con alcun tasto. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse.

L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a una coppia di key pair di riproduzione IVS, consulta TagResourceAmazon IVS Real-Time Streaming API Reference.

[IVS.2] Le configurazioni di registrazione IVS devono essere etichettate

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IVS::RecordingConfiguration`

Regola AWS Config : `ivs-recording configuration-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se una configurazione di registrazione Amazon IVS ha tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se la configurazione di registrazione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la configurazione di registrazione non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a una configurazione di registrazione IVS, consulta TagResourceAmazon IVS Real-Time Streaming API Reference.

[IVS.3] I canali IVS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IVS::Channel`

Regola AWS Config : `ivs-channel-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un canale Amazon IVS ha tag con le chiavi specifiche definite nel parametro`requiredKeyTags`. Il controllo fallisce se il canale non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il canale non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un canale IVS, consulta TagResourceAmazon IVS Real-Time Streaming API Reference.

Controlli CSPM di Security Hub per Amazon Keyspaces

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon Keyspaces.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Cassandra::Keyspace`

Regola AWS Config : `cassandra-keyspace-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se uno spazio di chiavi di Amazon Keyspaces contiene tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo fallisce se lo spazio delle chiavi non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredKeyTags` Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se lo spazio delle chiavi non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a uno spazio di chiavi di Amazon Keyspaces, consulta Aggiungere tag a uno spazio di chiavi nella Amazon Keyspaces Developer Guide.

Controlli CSPM Security Hub per Kinesis

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon Kinesis.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi

Requisiti correlati: 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), (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::Kinesis::Stream`

Regola AWS Config : kinesis-stream-encrypted

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i Kinesis Data Streams sono crittografati a riposo con la crittografia lato server. Questo controllo fallisce se un flusso Kinesis non è crittografato a riposo con la crittografia lato server.

Server-side la crittografia è una funzionalità di Amazon Kinesis Data Streams che crittografa automaticamente i dati prima che siano inattivi utilizzando un. AWS KMS key I dati vengono crittografati prima di essere scritti sul livello di archiviazione del flusso Kinesis e vengono decrittografati dopo essere stati recuperati dall'archiviazione. Di conseguenza, i tuoi dati vengono crittografati quando sono inattivi all'interno del servizio Amazon Kinesis Data Streams.

Correzione

Per informazioni sull'attivazione della crittografia lato server per gli stream Kinesis, vedi Come posso iniziare con la crittografia lato server? nella Amazon Kinesis Developer Guide.

[Kinesis.2] Gli stream Kinesis devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Kinesis::Stream`

AWS Config regola: `tagged-kinesis-stream` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un flusso di dati di Amazon Kinesis contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il flusso di dati non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro

`requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il flusso di dati non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un flusso di dati Kinesis, consulta Tagging your stream in Amazon Kinesis Data Streams nella Amazon Kinesis Developer Guide.

[Kinesis.3] I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato

Gravità: media

Tipo di risorsa: `AWS::Kinesis::Stream`

Regola AWS Config: kinesis-stream-backup-retention-check

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`minimumBackupRetentionPeriod`	Numero minimo di ore di conservazione dei dati.	Stringa	Da 24 a 8760	168

Questo controllo verifica se un flusso di dati di Amazon Kinesis ha un periodo di conservazione dei dati maggiore o uguale al periodo di tempo specificato. Il controllo fallisce se il periodo di conservazione dei dati è inferiore al periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione dei dati, Security Hub CSPM utilizza un valore predefinito di 168 ore.

In Kinesis Data Streams, un flusso di dati è una sequenza ordinata di record di dati pensati per essere scritti e letti in tempo reale. I record di dati vengono archiviati temporaneamente in frammenti del tuo stream. Il periodo di tempo dall'aggiunta di un record all'inaccessibilità viene chiamato il periodo di conservazione. Kinesis Data Streams rende quasi immediatamente inaccessibili i record più vecchi del nuovo periodo di conservazione dopo aver ridotto il periodo di conservazione. Ad esempio, modificando il periodo di conservazione da 24 ore a 48 ore significa che i record aggiunti al flusso 23 ore 55 minuti prima sono ancora disponibili dopo 24 ore.

Correzione

Per modificare il periodo di conservazione dei backup per Kinesis Data Streams, consulta Modifica del periodo di conservazione dei dati nella Amazon Kinesis Data Streams Developer Guide.

Controlli CSPM Security Hub per AWS KMS

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse AWS Key Management Service (AWS KMS). I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS

Requisiti correlati: 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), (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-05.01, Profilo CRI v2. 2/PR. AA-05.02, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::IAM::Policy`

Regola AWS Config : iam-customer-policy-blocked-kms-actions

Tipo di pianificazione: modifica attivata

Parametri:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(non personalizzabile)
- `excludePermissionBoundaryPolicy`: `True` (non personalizzabile)

Verifica se la versione predefinita delle policy gestite dai clienti di IAM consente ai responsabili di utilizzare le azioni di AWS KMS decrittografia su tutte le risorse. Il controllo fallisce se la policy è sufficientemente aperta da consentire `kms:ReEncryptFrom` azioni `kms:Decrypt` o azioni su tutte le chiavi KMS.

Il controllo controlla solo le chiavi KMS nell'elemento Resource e non tiene conto di eventuali condizioni nell'elemento Condition di una politica. Inoltre, il controllo valuta le politiche gestite dal cliente sia allegate che non collegate. Non verifica le politiche in linea o AWS le politiche gestite.

Con AWS KMS, puoi controllare chi può utilizzare le tue chiavi KMS e accedere ai tuoi dati crittografati. Le policy IAM definiscono quali azioni un'identità (utente, gruppo o ruolo) può eseguire su quali risorse. Seguendo le migliori pratiche di sicurezza, AWS consiglia di concedere il privilegio minimo. In altre parole, è necessario concedere alle identità solo le `kms:ReEncryptFrom` autorizzazioni `kms:Decrypt` or e solo le chiavi necessarie per eseguire un'operazione. In caso contrario, l'utente potrebbe utilizzare chiavi non appropriate per i dati.

Invece di concedere le autorizzazioni per tutte le chiavi, stabilisci il set minimo di chiavi di cui gli utenti hanno bisogno per accedere ai dati crittografati. Quindi progetta politiche che consentano agli utenti

di utilizzare solo quelle chiavi. Ad esempio, non consentite `kms:Decrypt` l'autorizzazione su tutte le chiavi KMS. Invece, consenti `kms:Decrypt` solo le chiavi in una particolare regione per il tuo account. Adottando il principio del privilegio minimo, puoi ridurre il rischio di divulgazione involontaria dei tuoi dati.

Correzione

Per modificare una policy gestita dai clienti IAM, consulta Modifica delle policy gestite dai clienti nella Guida per l'utente IAM. Quando modifichi la tua policy, per il `Resource` campo, fornisci l'Amazon Resource Name (ARN) della chiave o delle chiavi specifiche su cui desideri consentire le azioni di decrittografia.

[KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS

Requisiti correlati: 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, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.07

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Regola AWS Config : iam-inline-policy-blocked-kms-actions

Tipo di pianificazione: modifica attivata

Parametri:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(non personalizzabile)

Questo controllo verifica se le politiche in linea incorporate nelle identità IAM (ruolo, utente o gruppo) consentono le azioni di AWS KMS decrittografia e ricrittografia su tutte le chiavi KMS.

Il controllo fallisce se la policy è sufficientemente aperta da consentire azioni `kms:Decrypt` o `kms:ReEncryptFrom` azioni su tutte le chiavi KMS.

Il controllo controlla solo le chiavi KMS nell'elemento Resource e non tiene conto di eventuali condizioni nell'elemento Condition di una politica.

Con AWS KMS, puoi controllare chi può utilizzare le tue chiavi KMS e accedere ai tuoi dati crittografati. Le policy IAM definiscono quali azioni un'identità (utente, gruppo o ruolo) può eseguire su quali risorse. Seguendo le migliori pratiche di sicurezza, AWS consiglia di concedere il privilegio minimo. In altre parole, è necessario concedere alle identità solo le autorizzazioni necessarie e solo le chiavi necessarie per eseguire un'attività. In caso contrario, l'utente potrebbe utilizzare chiavi non appropriate per i dati.

Invece di concedere l'autorizzazione per tutte le chiavi, stabilisci il set minimo di chiavi di cui gli utenti hanno bisogno per accedere ai dati crittografati. Quindi progetta politiche che consentano agli utenti di utilizzare solo quelle chiavi. Ad esempio, non consentite `kms:Decrypt` l'autorizzazione su tutte le chiavi KMS. Consenti invece l'autorizzazione solo su chiavi specifiche in una regione specifica per il tuo account. Adottando il principio del privilegio minimo, puoi ridurre il rischio di divulgazione involontaria dei tuoi dati.

Correzione

Per modificare una policy in linea IAM, consulta Modifica delle policy in linea nella IAM User Guide. Quando modifichi la tua policy, per il `Resource` campo, fornisci l'Amazon Resource Name (ARN) della chiave o delle chiavi specifiche su cui desideri consentire le azioni di decrittografia.

[KMS.3] AWS KMS keys non devono essere eliminati involontariamente

Requisiti correlati: NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12 (2), CRI Profile v2. 2/PR. DS-01.02, Profilo CRI v2. 2/PR. PS-01.07

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Severità: critica

Tipo di risorsa: `AWS::KMS::Key`

AWS Config regola: `kms-cmk-not-scheduled-for-deletion-2` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la cancellazione delle chiavi KMS è pianificata. Il controllo ha esito negativo se è pianificata l'eliminazione di una chiave KMS.

Le chiavi KMS non possono essere recuperate una volta eliminate. I dati crittografati con una chiave KMS sono inoltre permanentemente irrecuperabili se la chiave KMS viene eliminata. Se i dati importanti sono stati crittografati con una chiave KMS programmata per l'eliminazione, prendi in considerazione la possibilità di decrittografare i dati o di ricrittografarli con una nuova chiave KMS, a meno che tu non stia eseguendo intenzionalmente una cancellazione crittografica.

Quando si pianifica l'eliminazione di una chiave KMS, viene imposto un periodo di attesa obbligatorio per consentire di annullare l'eliminazione, se è stata pianificata per errore. Il periodo di attesa predefinito è di 30 giorni, ma può essere ridotto a soli 7 giorni se è pianificata l'eliminazione della chiave KMS. Durante il periodo di attesa, l'eliminazione pianificata può essere annullata e la chiave KMS non verrà eliminata.

Per ulteriori informazioni sull'eliminazione delle chiavi KMS, consulta Eliminazione delle chiavi KMS nella Guida per gli sviluppatori.AWS Key Management Service

Correzione

Per annullare l'eliminazione pianificata di una chiave KMS, consulta Per annullare l'eliminazione di una chiave in Pianificazione e annullamento dell'eliminazione delle chiavi (console) nella Guida per gli sviluppatori.AWS Key Management Service

[KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/3.6, benchmark AWS CIS Foundations v3.0. 0/3.6, benchmark AWS CIS Foundations v1.4. 0/3.8, benchmark AWS CIS Foundations v1.2. 0/2.8, NIST.800-53.r5 SC-12 (2) NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-28 (3), PCI DSS versione 3.2. 1/36.4, PCI DSS versione 4.0. 1/3.7.4, Profilo CRI v2. 2/PR. PS-01.06, Profilo CRI v2. 2/PR. PS-01.07

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::KMS::Key`

Regola AWS Config : cmk-backing-key-rotation-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

AWS KMS consente ai clienti di ruotare la chiave di supporto, che è materiale chiave memorizzato AWS KMS ed è legato all'ID della chiave KMS. È la chiave di supporto utilizzata per eseguire operazioni di crittografia, ad esempio la crittografia e la decrittografia. Al momento, la rotazione automatica delle chiavi conserva tutte le chiavi di supporto precedenti, in modo che la decrittografia di dati crittografati possa essere eseguita in modo trasparente.

Il CIS consiglia di abilitare la rotazione delle chiavi KMS. La rotazione delle chiavi di crittografia consente di ridurre l'impatto potenziale di una chiave compromessa perché i dati crittografati con una nuova chiave non sono accessibili con una chiave precedente che potrebbe essere stata esposta.

Correzione

Per abilitare la rotazione delle chiavi KMS, consulta Come abilitare e disabilitare la rotazione automatica delle chiavi nella Guida per gli AWS Key Management Service sviluppatori.

[KMS.5] Le chiavi KMS non devono essere accessibili al pubblico

Requisiti correlati: CRI Profile v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. PS-01.07

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Severità: critica

Tipo di risorsa: `AWS::KMS::Key`

Regola AWS Config : kms-key-policy-no-public-access

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS KMS key è accessibile pubblicamente. Il controllo fallisce se la chiave KMS è accessibile pubblicamente.

L'implementazione dell'accesso con privilegi minimi è fondamentale per ridurre i rischi per la sicurezza e l'impatto di errori o intenzioni malevole. Se la policy chiave di an AWS KMS key consente l'accesso da account esterni, terze parti potrebbero essere in grado di crittografare e decrittografare i dati utilizzando la chiave. Ciò potrebbe comportare una minaccia interna o esterna che esfiltra i dati da Servizi AWS chi utilizza la chiave.

> **Note**
>
> Questo controllo restituisce inoltre un `FAILED` risultato che indica AWS KMS key se le configurazioni in uso AWS Config impediscono di registrare la politica della chiave nell'elemento di configurazione (CI) per la chiave KMS. AWS Config Per compilare la policy chiave nella CI per la chiave KMS, il AWS Config ruolo deve avere accesso alla lettura della policy chiave utilizzando la chiamata API. GetKeyPolicy Per risolvere questo tipo di `FAILED` risultato, verifica le politiche che possono impedire al AWS Config ruolo di accedere in lettura alla politica chiave per la chiave KMS. Ad esempio, controlla quanto segue:
>
> - La politica chiave per la chiave KMS.
> - Politiche di controllo dei servizi (SCP) e politiche di controllo delle risorse (RCP) AWS Organizations che si applicano al tuo account.
> - Autorizzazioni per il AWS Config ruolo, se non si utilizza il ruolo collegato al servizio.AWS Config
>
> Inoltre, questo controllo non valuta le condizioni delle policy che utilizzano caratteri jolly o variabili. Per produrre un `PASSED` risultato, le condizioni nella policy chiave devono utilizzare solo valori fissi, ossia valori che non contengono caratteri jolly o variabili di policy. Per informazioni sulle variabili di policy, consulta Variabili e tag nella Guida per l'AWS Identity and Access Management utente.

Correzione

Per informazioni sull'aggiornamento della politica chiave per un AWS KMS key, consulta le politiche chiave AWS KMS nella Guida per gli AWS Key Management Service sviluppatori.

Controlli CSPM Security Hub per AWS Lambda

Questi AWS Security Hub CSPM controlli valutano il AWS Lambda servizio e le risorse. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Lambda.1] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico

Requisiti correlati: 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. 1/1.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 1/7.2.1, PCI DSS versione 4.0. 1/7.2.1, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-04.01, Profilo CRI v2. 2/PR. AA-05.01

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: `AWS::Lambda::Function`

Regola AWS Config : lambda-function-public-access-prohibited

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la politica basata sulle risorse della funzione Lambda proibisce l'accesso pubblico all'esterno dell'account. Il controllo fallisce se è consentito l'accesso pubblico. Il controllo fallisce anche se una funzione Lambda viene richiamata da Amazon S3 e la policy non include una condizione per limitare l'accesso pubblico, ad esempio. `AWS:SourceAccount` Ti consigliamo di utilizzare altre condizioni S3 oltre alla tua policy sui bucket per un accesso più preciso. `AWS:SourceAccount`

> **Note**
>
> Questo controllo non valuta le condizioni delle policy che utilizzano caratteri jolly o variabili. Per produrre un `PASSED` risultato, le condizioni nella policy per la funzione Lambda devono utilizzare solo valori fissi, ossia valori che non contengono caratteri jolly o variabili di policy. Per informazioni sulle variabili di policy, consulta Variabili e tag nella Guida per l'AWS Identity and Access Management utente.

La funzione Lambda non dovrebbe essere accessibile al pubblico, in quanto ciò potrebbe consentire l'accesso involontario al codice della funzione.

Correzione

Per risolvere questo problema, è necessario aggiornare la politica basata sulle risorse della funzione per rimuovere le autorizzazioni o aggiungere la condizione. `AWS:SourceAccount` Puoi aggiornare la policy basata sulle risorse solo dall'API Lambda o. AWS CLI

Per iniziare, consulta la policy basata sulle risorse sulla console Lambda. Identifica la dichiarazione politica con valori di `Principal` campo che rendono pubblica la policy, ad esempio o. `"*"` `{ "AWS": "*" }`

Non è possibile modificare la policy dalla console. Per rimuovere le autorizzazioni dalla funzione, esegui il remove-permissioncomando da. AWS CLI

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

Sostituisci *<function-name>* con il nome della funzione Lambda e *<statement-id>* con l'istruzione ID (`Sid`) dell'istruzione che desideri rimuovere.

[Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati

Requisiti correlati: 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. 1/12.3.4, Profilo CRI v2. 2/PR. PS-02.01, Profilo CRI v2. 2/PR. PS-02.03

Categoria: Protezione > Sviluppo protetto

Gravità: media

Tipo di risorsa: `AWS::Lambda::Function`

Regola AWS Config : lambda-function-settings-check

Tipo di pianificazione: modifica attivata

Parametri:

- `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` (non personalizzabile)

Questo controllo verifica se le impostazioni di runtime della AWS Lambda funzione corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Il controllo fallisce se la funzione Lambda non utilizza un runtime supportato, come indicato nella sezione Parametri. Security Hub CSPM ignora le funzioni che hanno un tipo di pacchetto di. `Image`

I runtime Lambda si basano su una combinazione di sistema operativo, linguaggio di programmazione e librerie software soggette a manutenzione e aggiornamenti di sicurezza. Quando un componente di runtime non è più supportato per gli aggiornamenti di sicurezza, Lambda rende obsoleto il runtime. Anche se non è possibile creare funzioni che utilizzano il runtime obsoleto, la funzione è comunque disponibile per elaborare gli eventi di invocazione. Ti consigliamo di assicurarti che le tue funzioni Lambda siano aggiornate e non utilizzino ambienti di runtime obsoleti. Per un elenco dei runtime supportati, consulta i runtime Lambda nella AWS Lambda Developer Guide.

Correzione

Per ulteriori informazioni sui runtime e sulle pianificazioni di obsolescenza supportati, consulta la politica di deprecazione del runtime nella Developer Guide.AWS Lambda Quando esegui la migrazione dei runtime alla versione più recente, segui la sintassi e le indicazioni fornite dagli editori del linguaggio. Consigliamo inoltre di applicare gli aggiornamenti di runtime per ridurre il rischio di impatto sui carichi di lavoro nel raro caso di incompatibilità di una versione di runtime.

[Lambda.3] Le funzioni Lambda devono trovarsi in un VPC

Requisiti correlati: PCI DSS v3.2. 1/12.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 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 (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 (9), NIST.800-53.r5 SC-7 Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Configurazione di rete protetta

Gravità: bassa

Tipo di risorsa: `AWS::Lambda::Function`

AWS Config regola: lambda-inside-vpc

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una funzione Lambda è implementata in un cloud privato virtuale (VPC). Il controllo fallisce se la funzione Lambda non è distribuita in un VPC. Security Hub CSPM non valuta la configurazione del routing della sottorete VPC per determinare la raggiungibilità pubblica. È possibile che vengano visualizzati risultati non riusciti per le risorse Lambda @Edge.

L'implementazione di risorse in un VPC rafforza la sicurezza e il controllo sulle configurazioni di rete. Tali implementazioni offrono anche scalabilità e un'elevata tolleranza agli errori in più zone di disponibilità. È possibile personalizzare le implementazioni VPC per soddisfare diversi requisiti applicativi.

Correzione

Per configurare una funzione esistente per la connessione a sottoreti private nel tuo VPC, consulta Configuring VPC access nella Developer Guide.AWS Lambda Consigliamo di scegliere almeno due sottoreti private per un'elevata disponibilità e almeno un gruppo di sicurezza che soddisfi i requisiti di connettività della funzione.

[Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità

Requisiti correlati: 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/GV. RM-09.02, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::Lambda::Function`

Regola AWS Config : lambda-vpc-multi-az-check

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`availabilityZones`	Numero minimo di zone di disponibilità	Enum	`2, 3, 4, 5, 6`	2

Questo controllo verifica se una AWS Lambda funzione che si connette a un cloud privato virtuale (VPC) opera almeno nel numero specificato di zone di disponibilità (AZ). Il controllo fallisce se la funzione non funziona almeno nel numero specificato di AZ. A meno che non si fornisca un valore di parametro personalizzato per il numero minimo di AZ, Security Hub CSPM utilizza un valore predefinito di due AZ.

La distribuzione di risorse su più AZ è una AWS best practice per garantire un'elevata disponibilità all'interno dell'architettura. La disponibilità è un pilastro fondamentale del modello di sicurezza della triade di riservatezza, integrità e disponibilità. Tutte le funzioni Lambda che si connettono a un VPC devono disporre di un'implementazione Multi-AZ per garantire che una singola zona di errore non provochi un'interruzione totale delle operazioni.

Correzione

Se configuri la funzione per la connessione a un VPC nel tuo account, specifica le sottoreti in più AZ per garantire un'elevata disponibilità. Per istruzioni, consulta Configurazione dell'accesso al VPC nella Guida per AWS Lambda gli sviluppatori.

Lambda esegue automaticamente altre funzioni in più AZ per garantire che sia disponibile per elaborare gli eventi in caso di interruzione del servizio in una singola zona.

[Lambda.6] Le funzioni Lambda devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Lambda::Function`

AWS Config regola: `tagged-lambda-function` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se una AWS Lambda funzione ha tag con i tasti specifici definiti nel parametro. `requiredTagKeys` Il controllo fallisce se la funzione non ha alcuna chiave tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se la funzione non è etichettata con alcun tasto. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una funzione Lambda, consulta Using tags on Lambda functions nella Developer Guide.AWS Lambda

[Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato

Requisiti correlati: NIST.800-53.r5 CA-7, CRI Profile v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-04.02

Categoria: Identificazione > Registrazione

Gravità: bassa

Tipo di risorsa: `AWS::Lambda::Function`

Regola AWS Config : lambda-function-xray-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se active tracing with AWS X-Ray è abilitato per una AWS Lambda funzione. Il controllo fallisce se active tracing with X-Ray è disabilitato per la funzione Lambda.

AWS X-Ray può fornire funzionalità di tracciamento e monitoraggio delle AWS Lambda funzioni, che possono far risparmiare tempo e fatica nel debug e nell'utilizzo delle funzioni Lambda. Può aiutarti a diagnosticare gli errori e identificare rallentamenti, timeout e rallentamenti delle prestazioni suddividendo la latenza per le funzioni Lambda. Può anche aiutare con i requisiti di privacy e conformità dei dati. Se abiliti il tracciamento attivo per una funzione Lambda X-Ray, fornisce una visione olistica del flusso e dell'elaborazione dei dati all'interno della funzione Lambda, che può aiutarti a identificare potenziali vulnerabilità di sicurezza o pratiche di gestione dei dati non conformi. Questa visibilità può aiutarti a mantenere l'integrità, la riservatezza e la conformità dei dati alle normative pertinenti.

> **Note**
>
> AWS X-Ray il tracciamento non è attualmente supportato per le funzioni Lambda con Amazon Managed Streaming for Apache Kafka (Amazon MSK), Apache Kafka autogestito, Amazon MQ con ActiveMQ e RabbitMQ o mappature delle sorgenti di eventi Amazon DocumentDB.

Correzione

Per informazioni sull'abilitazione del tracciamento attivo per una AWS Lambda funzione, consulta Visualizza le chiamate alla funzione Lambda utilizzando nella Guida per gli sviluppatori. AWS X-RayAWS Lambda

Controlli CSPM Security Hub per Macie

Questi AWS Security Hub CSPM controlli valutano il servizio Amazon Macie.

Questi controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Macie.1] Amazon Macie dovrebbe essere abilitato

Requisiti correlati: 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, Profilo CRI v2. 2/ID. AM-05.02, Profilo CRI v2. 2/ID. AM-07.01, Profilo CRI v2. 2/PR. DS-01.02

Categoria: Rilevamento > Servizi di rilevamento

Gravità: media

Tipo di risorsa: `AWS:::Account`

Regola AWS Config : `macie-status-check`

Tipo di pianificazione: periodica

Questo controllo verifica se Amazon Macie è abilitato per un account. Il controllo fallisce se Macie non è abilitato per l'account.

Amazon Macie rileva i dati sensibili utilizzando l'apprendimento automatico e il pattern matching, fornisce visibilità sui rischi per la sicurezza dei dati e abilita la protezione automatizzata contro

tali rischi. Macie valuta automaticamente e continuamente i bucket Amazon Simple Storage Service (Amazon S3) per la sicurezza e il controllo degli accessi e genera risultati per informarti di potenziali problemi con la sicurezza o la privacy dei tuoi dati Amazon S3. Macie automatizza anche l'individuazione e la segnalazione di dati sensibili, come le informazioni di identificazione personale (PII), per fornirti una migliore comprensione dei dati archiviati in Amazon S3. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon Macie.

Correzione

Per abilitare Macie, consulta Enable Macie nella Guida per l'utente di Amazon Macie.

[Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato

Requisiti correlati: 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/PR. DS-01.02

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS:::Account`

Regola AWS Config : `macie-auto-sensitive-data-discovery-check`

Tipo di pianificazione: periodica

Questo controllo verifica se il rilevamento automatico di dati sensibili è abilitato per un account amministratore di Amazon Macie. Il controllo fallisce se il rilevamento automatico di dati sensibili non è abilitato per un account amministratore Macie. Questo controllo si applica solo agli account amministratore.

Macie automatizza il rilevamento e il reporting di dati sensibili, come le informazioni di identificazione personale (PII), nei bucket Amazon Simple Storage Service (Amazon S3). Grazie al rilevamento automatico dei dati sensibili, Macie valuta continuamente l'inventario dei bucket e utilizza tecniche di campionamento per identificare e selezionare oggetti S3 rappresentativi dai bucket. Macie analizza quindi gli oggetti selezionati, ispezionandoli alla ricerca di dati sensibili. Man mano che l'analisi procede, Macie aggiorna le statistiche, i dati di inventario e altre informazioni che fornisce sui dati S3. Macie genera anche risultati per segnalare i dati sensibili che trova.

Correzione

Per creare e configurare processi automatici di rilevamento di dati sensibili per analizzare oggetti nei bucket S3, consulta Configurazione del rilevamento automatico di dati sensibili per il tuo account nella Guida per l'utente di Amazon Macie.

Controlli CSPM del Security Hub per Amazon MSK

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon Managed Streaming for Apache Kafka (Amazon MSK). I controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker

Requisiti correlati: 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. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::MSK::Cluster`

Regola AWS Config : msk-in-cluster-node-require-tls

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon MSK è crittografato in transito con HTTPS (TLS) tra i nodi broker del cluster. Il controllo fallisce se è abilitata la comunicazione in testo semplice per una connessione al nodo del broker del cluster.

HTTPS offre un ulteriore livello di sicurezza in quanto utilizza TLS per spostare i dati e può essere utilizzato per impedire a potenziali aggressori di utilizzare attacchi person-in-the-middle o simili per intercettare o manipolare il traffico di rete. Per impostazione predefinita, Amazon MSK crittografa i dati in transito con TLS. Tuttavia, puoi ignorare questa impostazione predefinita al momento della creazione del cluster. Consigliamo di utilizzare connessioni crittografate tramite HTTPS (TLS) per le connessioni ai nodi del broker.

Correzione

Per informazioni sull'aggiornamento delle impostazioni di crittografia per un cluster Amazon MSK, consulta Updating security settings of a cluster nella Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato

Requisiti correlati: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. IR-04.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa: `AWS::MSK::Cluster`

Regola AWS Config : msk-enhanced-monitoring-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon MSK ha configurato il monitoraggio avanzato, specificato da un livello di monitoraggio di almeno`PER_TOPIC_PER_BROKER`. Il controllo fallisce se il livello di monitoraggio per il cluster è impostato su `DEFAULT` o`PER_BROKER`.

Il livello di `PER_TOPIC_PER_BROKER` monitoraggio fornisce informazioni più dettagliate sulle prestazioni del cluster MSK e fornisce anche metriche relative all'utilizzo delle risorse, come l'utilizzo della CPU e della memoria. Ciò consente di identificare i punti deboli in termini di prestazioni e i modelli di utilizzo delle risorse per singoli argomenti e broker. Questa visibilità, a sua volta, può ottimizzare le prestazioni dei vostri broker Kafka.

Correzione

Per configurare il monitoraggio avanzato per un cluster MSK, completa i seguenti passaggi:

1. Aprire la console Amazon MSK all'indirizzohttps://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Nel pannello di navigazione scegliere Cluster. Quindi, scegli un cluster.
3. Per Azione, seleziona Modifica monitoraggio.
4. Seleziona l'opzione per il monitoraggio avanzato a livello di argomento.

5. Scegli Save changes (Salva modifiche).

Per ulteriori informazioni sui livelli di monitoraggio, consulta i parametri di Amazon MSK per il monitoraggio dei broker Standard CloudWatch nella Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.3] I connettori MSK Connect devono essere crittografati in transito

Requisiti correlati: PCI DSS v4.0. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::KafkaConnect::Connector`

AWS Config regola: `msk-connect-connector-encrypted` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un connettore Amazon MSK Connect è crittografato in transito. Questo controllo fallisce se il connettore non è crittografato in transito.

I dati in transito si riferiscono ai dati che si spostano da una posizione all'altra, ad esempio tra i nodi del cluster o tra il cluster e l'applicazione. I dati possono spostarsi su Internet o all'interno di una rete privata. La crittografia dei dati in transito riduce il rischio che un utente non autorizzato possa intercettare il traffico di rete.

Correzione

È possibile abilitare la crittografia in transito quando si crea un connettore MSK Connect. Non è possibile modificare le impostazioni di crittografia dopo aver creato un connettore. Per ulteriori informazioni, consulta Creare un connettore nella Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato

Requisiti correlati: CRI Profile v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Gestione sicura degli accessi > Risorsa non accessibile al pubblico

Severità: critica

Tipo di risorsa: `AWS::MSK::Cluster`

Regola AWS Config : msk-cluster-public-access-disabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'accesso pubblico è disabilitato per un cluster Amazon MSK. Il controllo fallisce se l'accesso pubblico è abilitato per il cluster MSK.

Per impostazione predefinita, i client possono accedere a un cluster Amazon MSK solo se si trovano nello stesso VPC del cluster. Tutte le comunicazioni tra i client Kafka e un cluster MSK sono private per impostazione predefinita e i dati in streaming non attraversano Internet. Tuttavia, se un cluster MSK è configurato per consentire l'accesso pubblico, chiunque su Internet può stabilire una connessione ai broker Apache Kafka in esecuzione all'interno del cluster. Ciò può portare a problemi come l'accesso non autorizzato, la violazione dei dati o lo sfruttamento delle vulnerabilità. Se si limita l'accesso a un cluster richiedendo misure di autenticazione e autorizzazione, è possibile proteggere le informazioni sensibili e mantenere l'integrità delle risorse.

Correzione

Per informazioni sulla gestione dell'accesso pubblico a un cluster Amazon MSK, consulta Turn on public access to an MSK Provisioned cluster nella Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.5] I connettori MSK devono avere la registrazione abilitata

Requisiti correlati: CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/PR. PS-04.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::KafkaConnect::Connector`

Regola AWS Config : msk-connect-connector-logging-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione è abilitata per un connettore Amazon MSK. Il controllo fallisce se la registrazione è disabilitata per il connettore MSK.

I connettori Amazon MSK integrano sistemi esterni e servizi Amazon con Apache Kafka copiando continuamente i dati in streaming da una fonte di dati in un cluster Apache Kafka o copiando continuamente i dati da un cluster in un data sink. MSK Connect è in grado di scrivere eventi di registro che possono aiutare a eseguire il debug di un connettore. Quando crei un connettore, puoi specificare zero o più delle seguenti destinazioni di log: Amazon CloudWatch Logs, Amazon S3 e Amazon Data Firehose.

> **Note**
>
> Se un plug-in non definisce i valori di configurazione sensibili come segreti, tali valori possono apparire nei log dei connettori. Kafka Connect tratta i valori di configurazione non definiti allo stesso modo di qualsiasi altro valore non crittografato.

Correzione

Per abilitare la registrazione per un connettore Amazon MSK esistente, devi ricreare il connettore con la configurazione di registrazione appropriata. Per informazioni sulle opzioni di configurazione, consulta Logging for MSK Connect nella Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato

Requisiti correlati: CRI Profile v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-04.01, Profilo CRI v2. 2/PR. AA-05.02, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: `AWS::MSK::Cluster`

Regola AWS Config : msk-unrestricted-access-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'accesso non autenticato è abilitato per un cluster Amazon MSK. Il controllo fallisce se è abilitato l'accesso non autenticato per il cluster MSK.

Amazon MSK supporta i meccanismi di autenticazione e autorizzazione dei client per controllare l'accesso a un cluster. Questi meccanismi verificano l'identità dei client che si connettono al cluster e determinano le azioni che i client possono eseguire. Un cluster MSK può essere configurato per consentire l'accesso non autenticato, il che consente a qualsiasi client con connettività di rete di pubblicare e sottoscrivere argomenti di Kafka senza fornire credenziali. L'esecuzione di un cluster MSK senza richiedere l'autenticazione viola il principio del privilegio minimo e può esporre il cluster ad accessi non autorizzati. Può consentire a qualsiasi client di accedere, modificare o eliminare i dati relativi agli argomenti di Kafka, con conseguenti potenziali violazioni dei dati, modifiche non autorizzate dei dati o interruzioni del servizio. Consigliamo di abilitare meccanismi di autenticazione come l'autenticazione IAM o il TLS reciproco per garantire un controllo adeguato degli accessi e mantenere la conformità alla sicurezza. SASL/SCRAM

Correzione

Per informazioni sulla modifica delle impostazioni di autenticazione per un cluster Amazon MSK, consulta le seguenti sezioni della Amazon Managed Streaming for Apache Kafka Developer Guide: Aggiornamento delle impostazioni di sicurezza di un cluster Amazon MSK e Autenticazione e autorizzazione per le API Apache Kafka.

Controlli CSPM del Security Hub per Amazon MQ

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon MQ. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch

Requisiti correlati: NIST.800-53.r5 AU-2,, NIST.800-53.r5 AU-3 NIST.800-53.r5 AU-12, PCI DSS NIST.800-53.r5 SI-4 v4.0. 1/10.3.3, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::AmazonMQ::Broker`

Regola AWS Config : `mq-cloudwatch-audit-log-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un broker Amazon MQ ActiveMQ trasmette i log di audit ad Amazon Logs. CloudWatch Il controllo fallisce se il broker non trasmette i log di audit a Logs. CloudWatch

Pubblicando i log del broker ActiveMQ su Logs CloudWatch , è possibile CloudWatch creare allarmi e metriche che aumentano la visibilità delle informazioni relative alla sicurezza.

Correzione

Per trasmettere i log del broker ActiveMQ CloudWatch a Logs, consulta Configuring Amazon MQ for ActiveMQ logs nella Amazon MQ Developer Guide.

[MQ.4] I broker Amazon MQ devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::AmazonMQ::Broker`

AWS Config regola: `tagged-amazonmq-broker` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	I tag fanno distinzione tra maiuscole e minuscole			

Questo controllo verifica se un broker Amazon MQ dispone di tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il broker non dispone di chiavi di tag o se non dispone di tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il broker non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un broker Amazon MQ, consulta Tagging resources nella Amazon MQ Developer Guide.

[MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby

Requisiti correlati: 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), CRI Profile v2. 2/PR. IR-03.01

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: bassa

Tipo di risorsa: `AWS::AmazonMQ::Broker`

Regola AWS Config : `mq-active-deployment-mode`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la modalità di distribuzione per un broker Amazon MQ ActiveMQ è impostata su. active/standby Il controllo fallisce se come modalità di distribuzione è impostato un broker a istanza singola (abilitato per impostazione predefinita).

Active/standby l'implementazione offre un'elevata disponibilità per i broker Amazon MQ ActiveMQ in un. Regione AWS La modalità active/standby di implementazione include due istanze di broker in due diverse zone di disponibilità, configurate in una coppia ridondante. Questi broker comunicano in modo sincrono con l'applicazione, il che può ridurre i tempi di inattività e la perdita di dati in caso di guasto.

Correzione

Per creare un nuovo broker ActiveMQ active/standby con modalità di distribuzione, consulta Creazione e configurazione di un broker ActiveMQ nella Amazon MQ Developer Guide. Per la modalità di distribuzione, scegli broker. Active/standby Non puoi modificare la modalità di distribuzione per un broker esistente. È invece necessario creare un nuovo broker e copiare le impostazioni dal vecchio broker.

[MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster

Requisiti correlati: 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), CRI Profile v2. 2/GV. RM-09.02, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: bassa

Tipo di risorsa: `AWS::AmazonMQ::Broker`

Regola AWS Config : `mq-rabbit-deployment-mode`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la modalità di distribuzione per un broker Amazon MQ RabbitMQ è impostata sulla distribuzione in cluster. Il controllo fallisce se come modalità di distribuzione è impostato un broker a istanza singola (abilitato per impostazione predefinita).

La distribuzione in cluster offre un'elevata disponibilità per i broker Amazon MQ RabbitMQ in un unico. Regione AWS L'implementazione del cluster è un raggruppamento logico di tre nodi broker RabbitMQ, ciascuno con il proprio volume Amazon Elastic Block Store (Amazon EBS) e uno stato condiviso. L'implementazione del cluster garantisce la replica dei dati su tutti i nodi del cluster, il che può ridurre i tempi di inattività e la perdita di dati in caso di guasto.

Correzione

Per creare un nuovo broker RabbitMQ con modalità di distribuzione cluster, consulta Creazione e connessione a un broker RabbitMQ nella Amazon MQ Developer Guide. Per la modalità di distribuzione, scegli Distribuzione in cluster. Non è possibile modificare la modalità di distribuzione per un broker esistente. È invece necessario creare un nuovo broker e copiare le impostazioni dal vecchio broker.

Controlli CSPM del Security Hub per Neptune

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse di Amazon Neptune.

Questi controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi

Requisiti correlati: 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 Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `neptune-cluster-encrypted`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Neptune DB è crittografato quando è inattivo. Il controllo fallisce se un cluster Neptune DB non è crittografato a riposo.

I dati inattivi si riferiscono a tutti i dati archiviati in uno storage persistente e non volatile per qualsiasi durata. La crittografia aiuta a proteggere la riservatezza di tali dati, riducendo il rischio che un utente non autorizzato possa accedervi. La crittografia dei cluster Neptune DB protegge i dati e i metadati dall'accesso non autorizzato. Soddisfa inoltre i requisiti di conformità per la crittografia dei dati a riposo dei file system di produzione.

Correzione

È possibile abilitare la crittografia a riposo quando si crea un cluster Neptune DB. Non è possibile modificare le impostazioni di crittografia dopo aver creato un cluster. Per ulteriori informazioni, consulta Encrypting Neptune resources at rest nella Guida per l'utente di Neptune.

[Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch

Requisiti correlati: 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), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (5), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7(8), PCI DSS versione 4.0. 1/10.3.3, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `neptune-cluster-cloudwatch-log-export-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Neptune DB pubblica log di audit su Amazon Logs. CloudWatch Il controllo fallisce se un cluster Neptune DB non pubblica i log di controllo su Logs. CloudWatch `EnableCloudWatchLogsExport`dovrebbe essere impostato su. `Audit`

Amazon Neptune e CloudWatch Amazon sono integrati in modo da poter raccogliere e analizzare i parametri delle prestazioni. Neptune invia automaticamente le metriche e supporta anche gli CloudWatch allarmi. CloudWatch I log di controllo sono altamente personalizzabili. Quando si esegue l'audit di un database, ogni operazione sui dati può essere monitorata e registrata in una pista di controllo, incluse le informazioni su quale cluster di database si accede e in che modo. Ti consigliamo di inviare questi log per aiutarti CloudWatch a monitorare i cluster Neptune DB.

Correzione

Per pubblicare i log di controllo di Neptune su Logs CloudWatch , consulta Pubblicazione dei log di Neptune su Amazon Logs nella Neptune User Guide. CloudWatch Nella sezione Esportazioni dei log, scegli Audit.

[Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche

Requisiti correlati: 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, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Severità: critica

Tipo di risorsa: `AWS::RDS::DBClusterSnapshot`

Regola AWS Config : `neptune-cluster-snapshot-public-prohibited`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istantanea manuale del cluster DB di Neptune è pubblica. Il controllo fallisce se un'istantanea manuale del cluster DB di Neptune è pubblica.

Un'istantanea manuale del cluster Neptune DB non deve essere pubblica a meno che non sia prevista. Se condividi un'istantanea manuale non crittografata come pubblica, l'istantanea è disponibile per tutti. Account AWS Le istantanee pubbliche possono causare un'esposizione involontaria dei dati.

Correzione

Per rimuovere l'accesso pubblico alle istantanee manuali dei cluster DB di Neptune, consulta Condivisione di un'istantanea del cluster DB nella Guida per l'utente di Neptune.

[Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. DS-01.02, Profilo CRI v2. 2/PR. IR-03.01

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `neptune-cluster-deletion-protection-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Neptune DB ha la protezione da eliminazione abilitata. Il controllo fallisce se un cluster Neptune DB non ha la protezione da eliminazione abilitata.

L'attivazione della protezione da eliminazione del cluster offre un ulteriore livello di protezione contro l'eliminazione accidentale del database o l'eliminazione da parte di un utente non autorizzato. Un cluster Neptune DB non può essere eliminato mentre la protezione da eliminazione è abilitata. È necessario innanzitutto disabilitare la protezione da eliminazione prima che una richiesta di eliminazione possa avere successo.

Correzione

Per abilitare la protezione da eliminazione per un cluster Neptune DB esistente, consulta Modificare il cluster DB utilizzando la console, la CLI e l'API nella Guida per l'utente di Amazon Aurora.

[Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati

Requisiti correlati: NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-11.01, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02, Profilo CRI v2. 2/RC. RP-03.01

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `neptune-cluster-backup-retention-check`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`minimumBackupRetentionPeriod`	Periodo minimo di conservazione dei backup in giorni	Numero intero	Da 7 a 35	7	

Questo controllo verifica se un cluster Neptune DB ha abilitato i backup automatici e un periodo di conservazione dei backup maggiore o uguale al periodo di tempo specificato. Il controllo fallisce se i backup non sono abilitati per il cluster Neptune DB o se il periodo di conservazione è inferiore al periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione del backup, Security Hub CSPM utilizza un valore predefinito di 7 giorni.

I backup aiutano a ripristinare più rapidamente un incidente di sicurezza e a rafforzare la resilienza dei sistemi. Automatizzando i backup per i cluster Neptune DB, sarete in grado di ripristinare i sistemi in un determinato momento e ridurre al minimo i tempi di inattività e la perdita di dati.

Correzione

Per abilitare i backup automatici e impostare un periodo di conservazione dei backup per i cluster Neptune DB, consulta Enabling automatic backup nella Amazon RDS User Guide. Per il periodo di conservazione del Backup, scegli un valore maggiore o uguale a 7.

[Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive

Requisiti correlati: 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 Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBClusterSnapshot`

Regola AWS Config : `neptune-cluster-snapshot-encrypted`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istantanea del cluster Neptune DB è crittografata quando è inattiva. Il controllo fallisce se un cluster Neptune DB non è crittografato a riposo.

I dati inattivi si riferiscono a tutti i dati archiviati in uno storage persistente e non volatile per qualsiasi durata. La crittografia consente di proteggere la riservatezza di tali dati, riducendo il rischio che un utente non autorizzato possa accedervi. I dati nelle istantanee dei cluster Neptune DB devono essere crittografati quando sono inattivi per un ulteriore livello di sicurezza.

Correzione

Non è possibile crittografare uno snapshot del cluster Neptune DB esistente. È invece necessario ripristinare lo snapshot in un nuovo cluster DB e abilitare la crittografia sul cluster. È possibile creare un'istantanea crittografata dal cluster crittografato. Per istruzioni, consulta Ripristino da un'istantanea del cluster DB e Creazione di un'istantanea del cluster DB in Neptune nella Guida per l'utente di Neptune.

[Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata

Requisiti correlati: 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 Profile v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-05.02, Profilo CRI v2. 2/PR. PS-06.10

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `neptune-cluster-iam-database-authentication`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Neptune DB ha l'autenticazione del database IAM abilitata. Il controllo fallisce se l'autenticazione del database IAM non è abilitata per un cluster Neptune DB.

L'autenticazione del database IAM per i cluster di database Amazon Neptune elimina la necessità di memorizzare le credenziali degli utenti all'interno della configurazione del database perché l'autenticazione viene gestita esternamente tramite IAM. Quando l'autenticazione del database IAM è abilitata, ogni richiesta deve essere firmata utilizzando Signature Version 4. AWS

Correzione

Per impostazione predefinita, l'autenticazione del database IAM è disabilitata quando si crea un cluster Neptune DB. Per abilitarlo, consulta Enabling IAM database authentication in Neptune nella Neptune User Guide.

[Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee

Requisiti correlati: 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, Profilo CRI v2. 2/ID. AM-05.01, Profilo CRI v2. 2/ID. AM-08.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `neptune-cluster-copy-tags-to-snapshot-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Neptune DB è configurato per copiare tutti i tag nelle istantanee al momento della creazione delle istantanee. Il controllo fallisce se un cluster Neptune DB non è configurato per copiare i tag nelle istantanee.

L'identificazione e l'inventario delle risorse IT sono un aspetto cruciale della governance e della sicurezza. È necessario etichettare gli snapshot nello stesso modo dei relativi cluster di database Amazon RDS principali. La copia dei tag garantisce che i metadati per gli snapshot DB corrispondano a quelli dei cluster di database principali e che le politiche di accesso per lo snapshot DB corrispondano anche a quelle dell'istanza DB principale.

Correzione

Per copiare i tag nelle istantanee per i cluster Neptune DB, consulta Copiare i tag in Neptune nella Guida per l'utente di Neptune.

[Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `neptune-cluster-multi-az-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Neptune DB dispone di istanze di replica in lettura in più zone di disponibilità (AZ). Il controllo fallisce se il cluster viene distribuito in una sola AZ.

Se una AZ non è disponibile e durante gli eventi di manutenzione regolari, le repliche di lettura fungono da destinazioni di failover per l'istanza principale. Pertanto, se si verifica un errore nell'istanza primaria, Neptune promuove un'istanza di replica di lettura a diventare l'istanza primaria.

Al contrario, se il cluster DB non include istanze di replica in lettura, il cluster DB rimane non disponibile quando l'istanza primaria si guasta finché non viene ricreata. Re-creating l'istanza primaria impiega molto più tempo rispetto alla promozione di una replica di lettura. Per garantire un'elevata disponibilità, si consiglia di creare una o più istanze di replica di lettura che abbiano la stessa classe di istanza DB dell'istanza principale e si trovino in AZ diverse rispetto all'istanza principale.

Correzione

Per implementare un cluster Neptune DB in più AZ, consulta le istanze DB in un cluster Neptune Read-replica DB nella Guida per l'utente di Neptune.

Controlli CSPM Security Hub per AWS Network Firewall

Questi AWS Security Hub CSPM controlli valutano il AWS Network Firewall servizio e le risorse. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::NetworkFirewall::Firewall`

Regola AWS Config : netfw-multi-az-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo valuta se un firewall gestito tramite AWS Network Firewall è distribuito su più zone di disponibilità (AZ). Il controllo fallisce se un firewall viene distribuito in una sola AZ.

AWS l'infrastruttura globale ne include diverse Regioni AWS. Le AZ sono sedi fisicamente separate e isolate all'interno di ciascuna regione, collegate tramite reti a bassa latenza, ad alta velocità di trasmissione e altamente ridondanti. Implementando un firewall Network Firewall su più AZ, è possibile bilanciare e spostare il traffico tra le AZ, il che aiuta a progettare soluzioni ad alta disponibilità.

Correzione

Implementazione di un firewall Network Firewall su più AZ

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, in Network Firewall, scegli Firewall.
3. Nella pagina Firewall, seleziona il firewall che desideri modificare.
4. Nella pagina dei dettagli del firewall, scegli la scheda Dettagli del firewall.
5. Nella sezione Politica associata e VPC, scegli Modifica
6. Per aggiungere una nuova AZ, scegli Aggiungi nuova sottorete. Seleziona la AZ e la sottorete che desideri utilizzare. Assicurati di selezionare almeno due AZ.
7. Selezionare Salva.

[NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata

Requisiti correlati: 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), (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 (8) NIST.800-53.r5 SI-4, NIST.800-171.r2 3.1.20, NIST.800-53.r5 SI-7 NIST.800-171.r2 3.13.1, CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/PR. PS-04.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::NetworkFirewall::LoggingConfiguration`

Regola AWS Config : netfw-logging-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la registrazione è abilitata per un AWS Network Firewall firewall. Il controllo fallisce se la registrazione non è abilitata per almeno un tipo di registro o se la destinazione di registrazione non esiste.

La registrazione consente di mantenere l'affidabilità, la disponibilità e le prestazioni dei firewall. In Network Firewall, la registrazione fornisce informazioni dettagliate sul traffico di rete, tra cui l'ora in cui lo stateful engine ha ricevuto un flusso di pacchetti, informazioni dettagliate sul flusso di pacchetti e qualsiasi azione basata sullo stateful rule intrapresa contro il flusso di pacchetti.

Correzione

Per abilitare la registrazione per un firewall, consulta Aggiornamento della configurazione di registrazione di un firewall nella Guida per gli sviluppatori.AWS Network Firewall

[NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato

Requisiti correlati: 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 Profile v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02

Categoria: Protezione > Configurazione di rete sicura

Gravità: media

Tipo di risorsa: `AWS::NetworkFirewall::FirewallPolicy`

Regola AWS Config : netfw-policy-rule-group-associated

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se a una policy Network Firewall sono associati gruppi di regole stateful o stateless. Il controllo ha esito negativo se non vengono assegnati gruppi di regole stateless o stateful.

Una policy firewall definisce il modo in cui il firewall monitora e gestisce il traffico in Amazon Virtual Private Cloud (Amazon VPC). La configurazione di gruppi di regole stateless e stateful aiuta a filtrare pacchetti e flussi di traffico e definisce la gestione del traffico predefinita.

Correzione

Per aggiungere un gruppo di regole a una policy Network Firewall, vedere Aggiornamento di una policy firewall nella AWS Network Firewall Developer Guide. Per informazioni sulla creazione e la gestione dei gruppi di regole, consulta Gruppi di regole in AWS Network Firewall.

[NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/PR. IR-01.02

Categoria: Protezione > Configurazione di rete sicura

Gravità: media

Tipo di risorsa: `AWS::NetworkFirewall::FirewallPolicy`

Regola AWS Config : netfw-policy-default-action-full-packets

Tipo di pianificazione: modifica attivata

Parametri:

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe`(non personalizzabile)

Questo controllo verifica se l'azione stateless predefinita per pacchetti completi per una policy Network Firewall è drop o forward. Il controllo passa se è selezionato `Drop` o `Forward` è selezionato e fallisce se `Pass` è selezionato.

Una policy firewall definisce il modo in cui il firewall monitora e gestisce il traffico in Amazon VPC. Puoi configurare gruppi di regole stateless e stateful per filtrare pacchetti e flussi di traffico. L'impostazione predefinita è in grado `Pass` di consentire il traffico non intenzionale.

Correzione

Per modificare la politica del firewall, consulta Aggiornamento di una politica del firewall nella Guida per gli sviluppatori.AWS Network Firewall Per le azioni predefinite Stateless, scegli Modifica. Quindi, scegli Elimina o Inoltra ai gruppi di regole con stato come Azione.

[NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.14 NIST.800-53.r5 CM-2, 3.13.1, NIST.800-171.r2 3.13.6, CRI Profile v2. NIST.800-171.r2 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. IR-01.03

Categoria: Protezione > Configurazione di rete sicura

Gravità: media

Tipo di risorsa: `AWS::NetworkFirewall::FirewallPolicy`

Regola AWS Config : netfw-policy-default-action-fragment-packets

Tipo di pianificazione: modifica attivata

Parametri:

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe`(non personalizzabile)

Questo controllo verifica se l'azione stateless predefinita per i pacchetti frammentati per una policy Network Firewall è drop o forward. Il controllo passa se è selezionato `Drop` o `Forward` è selezionato e fallisce se `Pass` è selezionato.

Una policy firewall definisce il modo in cui il firewall monitora e gestisce il traffico in Amazon VPC. Puoi configurare gruppi di regole stateless e stateful per filtrare pacchetti e flussi di traffico. L'impostazione predefinita è in grado `Pass` di consentire il traffico non intenzionale.

Correzione

Per modificare la politica del firewall, consulta Aggiornamento di una politica del firewall nella Guida per gli sviluppatori.AWS Network Firewall Per le azioni predefinite Stateless, scegli Modifica. Quindi, scegli Elimina o Inoltra ai gruppi di regole con stato come Azione.

[NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto

Requisiti correlati: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (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, Profilo CRI v2. 2/DE. CM-01.05

Categoria: Protezione > Configurazione di rete sicura

Gravità: media

Tipo di risorsa: `AWS::NetworkFirewall::RuleGroup`

Regola AWS Config : netfw-stateless-rule-group-not-empty

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo di regole senza stato in AWS Network Firewall contiene regole. Il controllo ha esito negativo se non ci sono regole nel gruppo di regole.

Un gruppo di regole contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, potrebbe dare l'impressione che il gruppo di regole elabori il traffico. Tuttavia, quando il gruppo di regole stateless è vuoto, non elabora il traffico.

Correzione

Per aggiungere regole al gruppo di regole Network Firewall, consulta Aggiornamento di un gruppo di regole stateful nella Guida per gli AWS Network Firewall sviluppatori. Nella pagina dei dettagli del firewall, per il gruppo di regole Stateless, scegli Modifica per aggiungere regole.

[NetworkFirewall.7] I firewall Network Firewall devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::NetworkFirewall::Firewall`

AWS Config regola: `tagged-networkfirewall-firewall` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfan	`No default value`

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	I tag fanno distinzione tra maiuscole e minuscole		o i requisiti AWS .	

Questo controllo verifica se un AWS Network Firewall firewall dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il firewall non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il firewall non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un firewall Network Firewall, consulta Tagging AWS Network Firewall resources nella AWS Network Firewall Developer Guide.

[NetworkFirewall.8] Le politiche firewall di Network Firewall devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config regola: `tagged-networkfirewall-firewallpolicy` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se una policy AWS Network Firewall firewall contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la politica del firewall non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la politica del firewall non è contrassegnata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una politica di Network Firewall, consulta Tagging AWS Network Firewall resources nella AWS Network Firewall Developer Guide.

[NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata

Requisiti correlati: 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. IR-01.02

Categoria: Protezione > Sicurezza di rete

Gravità: media

Tipo di risorsa: `AWS::NetworkFirewall::Firewall`

Regola AWS Config : netfw-deletion-protection-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS Network Firewall firewall ha la protezione da eliminazione abilitata. Il controllo fallisce se la protezione da eliminazione non è abilitata per un firewall.

AWS Network Firewall è un firewall di rete gestito a stato e un servizio di rilevamento delle intrusioni che consente di ispezionare e filtrare il traffico da, verso o tra i Virtual Private Cloud (VPC). L'impostazione di protezione dall'eliminazione protegge dall'eliminazione accidentale del firewall.

Correzione

Per abilitare la protezione da eliminazione su un firewall Network Firewall esistente, vedere Aggiornamento di un firewall nella AWS Network Firewall Developer Guide. Per Modifica le protezioni, seleziona Abilita. Puoi anche abilitare la protezione dall'eliminazione richiamando l' UpdateFirewallDeleteProtectionAPI e impostando il `DeleteProtection` campo su. `true`

[NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Sicurezza di rete

Gravità: media

Tipo di risorsa: `AWS::NetworkFirewall::Firewall`

Regola AWS Config : netfw-subnet-change-protection-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la protezione da modifica della sottorete è abilitata per un AWS Network Firewall firewall. Il controllo fallisce se la protezione da modifica della sottorete non è abilitata per il firewall.

AWS Network Firewall è un firewall di rete gestito e dotato di stato e un servizio di rilevamento delle intrusioni che puoi utilizzare per ispezionare e filtrare il traffico da, verso o tra i tuoi Virtual Private Cloud (VPC). Se si abilita la protezione da modifiche di sottorete per un firewall Network Firewall, è possibile proteggere il firewall da modifiche accidentali alle associazioni di sottorete del firewall.

Correzione

Per informazioni sull'attivazione della protezione da modifiche di sottorete per un firewall Network Firewall esistente, vedere Updating a firewall nella AWS Network Firewall Developer Guide.

Controlli CSPM di Security Hub per Amazon Service OpenSearch

Questi AWS Security Hub CSPM controlli valutano il OpenSearch servizio e le risorse di Amazon OpenSearch Service (Service). I controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata

Requisiti correlati: PCI DSS v3.2. 1/12.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 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 (6), Profilo CRI NIST.800-53.r5 SI-7 v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::OpenSearch::Domain`

Regola AWS Config : `opensearch-encrypted-at-rest`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se nei OpenSearch domini è abilitata la configurazione di crittografia a riposo. Il controllo non riesce se la crittografia dei dati inattivi non è abilitata.

Per un ulteriore livello di sicurezza per i dati sensibili, è necessario configurare il dominio di OpenSearch servizio in modo che venga crittografato quando non è attivo. Quando configuri la crittografia dei dati inattivi, AWS KMS archivia e gestisce le chiavi di crittografia. Per eseguire la crittografia, AWS KMS utilizza l'algoritmo Advanced Encryption Standard con chiavi a 256 bit ()AES-256.

Per ulteriori informazioni sulla crittografia dei OpenSearch servizi a riposo, consulta Encryption of data at rest for Amazon OpenSearch Service nella Amazon OpenSearch Service Developer Guide.

Correzione

Per abilitare la crittografia a riposo per OpenSearch domini nuovi ed esistenti, consulta Enabling encryption of data at rest nella Amazon OpenSearch Service Developer Guide.

[Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico

Requisiti correlati: PCI DSS v3.2. 1/12.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 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 (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), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 Profilo CRI v2. 2/PR. IR-01.01

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Severità: critica

Tipo di risorsa: `AWS::OpenSearch::Domain`

Regola AWS Config : `opensearch-in-vpc-only`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i OpenSearch domini si trovano in un VPC. Non valuta la configurazione del routing della sottorete VPC per determinare l'accesso pubblico.

È necessario assicurarsi che i OpenSearch domini non siano collegati a sottoreti pubbliche. Consulta Resource-based le politiche nell'Amazon OpenSearch Service Developer Guide. È inoltre necessario assicurarsi che il VPC sia configurato in base alle procedure consigliate. Consulta le best practice di sicurezza per il tuo VPC nella Amazon VPC User Guide.

OpenSearch i domini distribuiti all'interno di un VPC possono comunicare con le risorse VPC sulla AWS rete privata, senza la necessità di attraversare la rete Internet pubblica. Questa configurazione aumenta il livello di sicurezza limitando l'accesso ai dati in transito. I VPC forniscono una serie di controlli di rete per proteggere l'accesso ai OpenSearch domini, inclusi l'ACL di rete e i gruppi di sicurezza. Security Hub consiglia di migrare OpenSearch i domini pubblici ai VPC per sfruttare questi controlli.

Correzione

Se si crea un dominio con un endpoint pubblico, non è possibile inserirlo in un VPC in un secondo momento. Devi invece creare un nuovo dominio ed eseguire la migrazione dei dati. È vero anche il

contrario. Se si crea un dominio all'interno di un VPC, non può avere un endpoint pubblico. È invece necessario creare un altro dominio o disabilitare questo controllo.

Per istruzioni, consulta Launching your Amazon OpenSearch Service domain all'interno di un VPC nella Amazon OpenSearch Service Developer Guide.

[Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi

Requisiti correlati: 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), CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. IR-01.05, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::OpenSearch::Domain`

Regola AWS Config : `opensearch-node-to-node-encryption-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se nei OpenSearch domini è abilitata la crittografia da nodo a nodo. Questo controllo ha esito negativo se la crittografia da nodo a nodo è disabilitata nel dominio.

HTTPS (TLS) può essere utilizzato per impedire a potenziali aggressori di intercettare o manipolare il traffico di rete utilizzando attacchi person-in-the-middle o simili. Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS). L'abilitazione della crittografia da nodo a nodo per i domini garantisce che le comunicazioni all'interno del cluster siano crittografate durante il transito. OpenSearch

Questa configurazione può comportare un calo delle prestazioni. È necessario conoscere e testare il compromesso in termini di prestazioni prima di attivare questa opzione.

Correzione

Per abilitare la crittografia da nodo a nodo su un OpenSearch dominio, consulta Enabling node-to-node encryption nella Amazon Service Developer Guide. OpenSearch

[Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch

Requisiti correlati: 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), CRI Profile v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::OpenSearch::Domain`

Regola AWS Config : `opensearch-logs-to-cloudwatch`

Tipo di pianificazione: modifica attivata

Parametri:

- `logtype = 'error'`(non personalizzabile)

Questo controllo verifica se i OpenSearch domini sono configurati per inviare i log degli errori ai CloudWatch registri. Questo controllo ha esito negativo se la registrazione degli errori non CloudWatch è abilitata per un dominio.

È necessario abilitare i log degli errori per i OpenSearch domini e inviarli a Logs per la conservazione e la CloudWatch risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

Correzione

Per abilitare la pubblicazione dei log, consulta Enabling log publishing (console) nella Amazon OpenSearch Service Developer Guide.

[Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata

Requisiti correlati: 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. 1/10.2.1, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::OpenSearch::Domain`

Regola AWS Config : `opensearch-audit-logging-enabled`

Tipo di pianificazione: modifica attivata

Parametri:

- `cloudWatchLogsLogGroupArnList`(non personalizzabile) — Security Hub CSPM non compila questo parametro. Comma-separated elenco di gruppi di CloudWatch log che devono essere configurati per i log di controllo.

Questo controllo verifica se nei OpenSearch domini è abilitata la registrazione di controllo. Questo controllo ha esito negativo se in un OpenSearch dominio non è abilitata la registrazione di controllo.

I log di controllo sono altamente personalizzabili. Ti consentono di tenere traccia delle attività degli utenti sui tuoi OpenSearch cluster, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le OpenSearch query di ricerca in arrivo.

Correzione

Per istruzioni su come abilitare i log di controllo, consulta Enabling audit logs nella Amazon OpenSearch Service Developer Guide.

[Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::OpenSearch::Domain`

Regola AWS Config : `opensearch-data-node-fault-tolerance`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i OpenSearch domini sono configurati con almeno tre nodi di dati e `zoneAwarenessEnabled` lo è. `true` Questo controllo ha esito negativo per un OpenSearch dominio se `instanceCount` è inferiore a 3 o lo `zoneAwarenessEnabled` è`false`.

Per ottenere disponibilità e tolleranza agli errori elevate a livello di cluster, un OpenSearch dominio deve avere almeno tre nodi di dati. L'implementazione di un OpenSearch dominio con almeno tre nodi di dati garantisce le operazioni del cluster in caso di guasto di un nodo.

Correzione

Per modificare il numero di nodi di dati in un dominio OpenSearch

1. Accedi alla AWS console e apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/.
2. In I miei domini, scegli il nome del dominio da modificare e scegli Modifica.
3. In Nodi dati imposta Numero di nodi su un numero maggiore di`3`. Se esegui la distribuzione in tre zone di disponibilità, imposta il numero su un multiplo di tre per garantire una distribuzione equa tra le zone di disponibilità.
4. Seleziona Invia.

[Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato

Requisiti correlati: 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),,, CRI Profile NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6 v2. 2/DE. CM-03.01, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03, Profilo CRI v2. 2/PR. PS-04.02

Categoria: Protezione > Gestione degli accessi sicuri > Azioni API sensibili limitate

Gravità: alta

Tipo di risorsa: `AWS::OpenSearch::Domain`

Regola AWS Config : `opensearch-access-control-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se nei OpenSearch domini è abilitato il controllo granulare degli accessi. Il controllo fallisce se il controllo di accesso a grana fine non è abilitato. Fine-grained il controllo degli accessi richiede che `advanced-security-options` il OpenSearch parametro sia abilitatou`pdate-domain-config`.

Fine-grained il controllo degli accessi offre modi aggiuntivi per controllare l'accesso ai tuoi dati su Amazon OpenSearch Service.

Correzione

Per abilitare un controllo granulare degli accessi, consulta il controllo degli Fine-grained accessi in Amazon Service nella Amazon OpenSearch Service Developer Guide OpenSearch .

[Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente

Requisiti correlati: 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), CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. IR-01.05, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::OpenSearch::Domain`

Regola AWS Config : `opensearch-https-required`

Tipo di pianificazione: modifica attivata

Parametri:

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10`(non personalizzabile)

Questo controllo verifica se un endpoint di dominio Amazon OpenSearch Service è configurato per utilizzare la politica di sicurezza TLS più recente. Il controllo fallisce se l'endpoint del OpenSearch dominio non è configurato per utilizzare la politica supportata più recente o se HTTPS non è abilitato.

Puoi utilizzare HTTPS (TLS) per impedire a potenziali aggressori di utilizzare attacchi di tipo person-in-the-middle o simili per intercettare o manipolare traffico di rete. Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS). La crittografia dei dati in transito può influire sulle prestazioni. È consigliabile testare l'applicazione con questa funzionalità per comprendere il profilo delle prestazioni e l'impatto del TLS. TLS 1.2 offre diversi miglioramenti della sicurezza rispetto alle versioni precedenti di TLS.

Correzione

Per abilitare la crittografia TLS, utilizza l'operazione API. UpdateDomainConfig Configura il DomainEndpointOptionscampo per specificare il valore per`TLSSecurityPolicy`. Per ulteriori informazioni, consulta la sezione sulla Node-to-node crittografia nell'Amazon OpenSearch Service Developer Guide.

[Opensearch.9] i OpenSearch domini devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::OpenSearch::Domain`

AWS Config regola: `tagged-opensearch-domain` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfan	`No default value`

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
	I tag fanno distinzione tra maiuscole e minuscole		o i requisiti AWS .	

Questo controllo verifica se un dominio Amazon OpenSearch Service ha tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il dominio non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il dominio non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un dominio OpenSearch di servizio, consulta Working with tags nella Amazon OpenSearch Service Developer Guide.

[Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software

Requisiti correlati: 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. 1/6.3.3, Profilo CRI v2. 2/ID. RA-01.03, Profilo CRI v2. 2/PR. PS-02.01

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: `AWS::OpenSearch::Domain`

Regola AWS Config : `opensearch-update-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se in un dominio Amazon OpenSearch Service è installato l'ultimo aggiornamento software. Il controllo fallisce se un aggiornamento software è disponibile ma non è installato per il dominio.

OpenSearch Gli aggiornamenti del software di servizio forniscono le correzioni, gli aggiornamenti e le funzionalità più recenti della piattaforma disponibili per l'ambiente. Mantenersi aggiornati sull'installazione delle patch aiuta a mantenere la sicurezza e la disponibilità del dominio. Se non viene intrapresa alcuna azione sugli aggiornamenti richiesti, il software di servizio viene aggiornato automaticamente (in genere dopo 2 settimane). Ti consigliamo di pianificare gli aggiornamenti in un periodo di scarso traffico verso il dominio per ridurre al minimo le interruzioni del servizio.

Correzione

Per installare gli aggiornamenti software per un OpenSearch dominio, consulta Starting an update nella Amazon OpenSearch Service Developer Guide.

[Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: bassa

Tipo di risorsa: `AWS::OpenSearch::Domain`

Regola AWS Config : `opensearch-primary-node-fault-tolerance`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un dominio Amazon OpenSearch Service è configurato con almeno tre nodi primari dedicati. Il controllo fallisce se il dominio ha meno di tre nodi primari dedicati.

OpenSearch Il servizio utilizza nodi primari dedicati per aumentare la stabilità del cluster. Un nodo primario dedicato esegue attività di gestione del cluster, ma non contiene dati né risponde alle richieste di caricamento dei dati. Si consiglia di utilizzare Multi-AZ con standby, che aggiunge tre nodi primari dedicati a ciascun dominio di produzione OpenSearch .

Correzione

Per modificare il numero di nodi primari per un OpenSearch dominio, consulta Creazione e gestione dei domini Amazon OpenSearch Service nella Amazon OpenSearch Service Developer Guide.

Controlli CSPM Security Hub per AWS Private CA

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse AWS Autorità di certificazione privata (AWS Private CA).

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/PR. PS-01.07

Categoria: Protezione > Configurazione di rete protetta

Gravità: bassa

Tipo di risorsa: `AWS::ACMPCA::CertificateAuthority`

Regola AWS Config : `acm-pca-root-ca-disabled`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se AWS Private CA dispone di un'autorità di certificazione (CA) principale disabilitata. Il controllo fallisce se la CA principale è abilitata.

Con AWS Private CA, è possibile creare una gerarchia di CA che include una CA radice e CA subordinate. È necessario ridurre al minimo l'uso della CA principale per le attività quotidiane, specialmente negli ambienti di produzione. La CA principale deve essere utilizzata solo per emettere certificati per CA intermedie. Ciò consente alla CA root di essere archiviata in modo sicuro mentre le CA intermedie eseguono l'attività quotidiana di emissione di certificati di entità finale.

Correzione

Per disabilitare la CA principale, consulta la sezione Aggiornamento dello stato della CA nella Guida per l'AWS Autorità di certificazione privata utente.

[PCA.2] AWS Le autorità di certificazione CA private devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::ACMPCA::CertificateAuthority`

Regola AWS Config : `acmpca-certificate-authority-tagged`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un'autorità di certificazione CA AWS privata dispone di tag con le chiavi specifiche definite nel parametro. `requiredKeyTags` Il controllo ha esito negativo se l'autorità di certificazione non dispone di chiavi di tag o se non dispone di tutte le chiavi specificate nel parametro`requiredKeyTags`. Se il parametro `requiredKeyTags` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'autorità di certificazione non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella Guida per l'utente IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Correzione

Per aggiungere tag a un'autorità CA AWS privata, consulta Aggiungere tag per la CA privata nella Guida per l'AWS Autorità di certificazione privata utente.

Controlli CSPM del Security Hub per Amazon RDS

Questi AWS Security Hub CSPM controlli valutano le risorse di Amazon Relational Database Service (Amazon RDS) e Amazon RDS. I controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[RDS.1] L'istantanea RDS deve essere privata

Requisiti correlati: PCI DSS v3.2. 1/12.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 1/1.3.6, PCI DSS versione 3.2. 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), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa:`AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

Regola AWS Config : `rds-snapshots-public-prohibited`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se gli snapshot di Amazon RDS sono pubblici. Il controllo fallisce se le istantanee RDS sono pubbliche. Questo controllo valuta le istanze RDS, le istanze Aurora DB, le istanze Neptune DB e i cluster Amazon DocumentDB.

Gli snapshot RDS vengono utilizzati per eseguire il backup dei dati nelle istanze RDS in un determinato momento. Possono essere utilizzati per ripristinare gli stati precedenti delle istanze RDS.

Uno snapshot RDS non deve essere pubblico a meno che non sia previsto. Se condividi uno snapshot manuale non crittografato come pubblico, questo rende lo snapshot disponibile a tutti. Account AWS Ciò potrebbe comportare l'esposizione non intenzionale dei dati dell'istanza RDS.

Tieni presente che se la configurazione viene modificata per consentire l'accesso pubblico, la AWS Config regola potrebbe non essere in grado di rilevare la modifica per un massimo di 12 ore. Finché la AWS Config regola non rileva la modifica, il controllo viene superato anche se la configurazione viola la regola.

Per ulteriori informazioni sulla condivisione di uno snapshot DB, consulta Sharing a DB snapshot nella Amazon RDS User Guide.

Correzione

Per rimuovere l'accesso pubblico dagli snapshot RDS, consulta Sharing a snapshot nella Amazon RDS User Guide. Per la visibilità degli snapshot DB, scegliamo Private.

[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/2.2.3, benchmark AWS CIS Foundations v3.0. 0/2.3.3 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (11) 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 (5), NIST.800-53.r5 SC-7 PCI DSS versione 3.2. 1/1.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 1/1.3.6, PCI DSS versione 3.2. 1/7.2.1, PCI DSS versione 4.0. 1/1.4.4, Profilo CRI v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. IR-01.01

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : `rds-instance-public-access-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le istanze di Amazon RDS sono accessibili al pubblico valutando il `PubliclyAccessible` campo nell'elemento di configurazione dell'istanza.

Il valore `PubliclyAccessible` nella configurazione dell'istanza RDS indica se l'istanza database è accessibile pubblicamente. Quando l'istanza DB è configurata con`PubliclyAccessible`, è un' Internet-facing istanza con un nome DNS risolvibile pubblicamente, che si risolve in un indirizzo IP pubblico. Quando l'istanza database non è accessibile pubblicamente, è un'istanza interna con un nome DNS che si risolve in un indirizzo IP privato.

A meno che non si intenda rendere l'istanza RDS accessibile al pubblico, l'istanza RDS non deve essere configurata con valore. `PubliclyAccessible` In questo modo si potrebbe consentire un traffico non necessario verso l'istanza del database.

Correzione

Per rimuovere l'accesso pubblico dalle istanze DB RDS, consulta Modificare un'istanza DB Amazon RDS nella Amazon RDS User Guide. Per l'accesso pubblico, scegli No.

[RDS.3] Le istanze DB RDS devono avere la crittografia a riposo abilitata

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/2.2.1, benchmark AWS CIS Foundations v3.0. 0/2.3.1, benchmark AWS CIS Foundations v1.4. 0/2.3.1, 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 (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : `rds-storage-encrypted`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la crittografia dello storage è abilitata per le istanze database di Amazon RDS.

Questo controllo è destinato alle istanze DB RDS. Tuttavia, può anche generare risultati per le istanze Aurora DB, le istanze Neptune DB e i cluster Amazon DocumentDB. Se questi risultati non sono utili, puoi eliminarli.

Per un ulteriore livello di sicurezza per i dati sensibili nelle istanze database RDS è necessario configurare la crittografia dei dati inattivi delle istanze database RDS. Per crittografare i dati inattivi delle istanze database RDS e degli snapshot, abilita l'opzione di crittografia per le istanze database RDS. I dati che vengono crittografati quando sono inattivi includono lo storage sottostante per le istanze database, i backup automatici, le repliche di lettura e gli snapshot.

Le istanze DB crittografate con RDS utilizzano l'algoritmo di AES-256 crittografia standard aperto per crittografare i dati sul server che ospita le istanze DB RDS. Dopo la crittografia dei dati, Amazon RDS gestisce l'autenticazione dell'accesso e la decrittografia dei dati in modo trasparente con un impatto

minimo sulle prestazioni. Non è quindi necessario modificare le applicazioni client di database per utilizzare la crittografia.

La crittografia Amazon RDS è attualmente disponibile per tutti i motori di database e i tipi di storage. La crittografia Amazon RDS è disponibile per la maggior parte delle classi di istanza database. Per informazioni sulle classi di istanze DB che non supportano la crittografia Amazon RDS, consulta Encrypting Amazon RDS resources nella Amazon RDS User Guide.

Correzione

Per informazioni sulla crittografia delle istanze DB in Amazon RDS, consulta Encrypting Amazon RDS resources nella Amazon RDS User Guide.

[RDS.4] Gli snapshot del cluster RDS e gli snapshot del database devono essere crittografati quando sono inattivi

Requisiti correlati: 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 Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa:, `AWS::RDS::DBClusterSnapshot` `AWS::RDS::DBSnapshot`

Regola AWS Config : `rds-snapshot-encrypted`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istantanea di RDS DB è crittografata. Il controllo ha esito negativo se uno snapshot RDS DB non è crittografato.

Questo controllo è destinato alle istanze DB RDS. Tuttavia, può anche generare risultati per istantanee di istanze Aurora DB, istanze DB Neptune e cluster Amazon DocumentDB. Se questi risultati non sono utili, puoi eliminarli.

La crittografia dei dati inattivi riduce il rischio che un utente non autenticato acceda ai dati archiviati su disco. I dati nelle istantanee RDS devono essere crittografati quando sono inattivi per un ulteriore livello di sicurezza.

Correzione

Per crittografare uno snapshot RDS, consulta Encrypting Amazon RDS resources nella Amazon RDS User Guide. Quando crittografi un'istanza DB RDS, i dati crittografati includono lo storage sottostante dell'istanza, i relativi backup automatici, le repliche di lettura e le istantanee.

È possibile crittografare un'istanza DB RDS solo al momento della creazione, non dopo la creazione dell'istanza DB. Tuttavia, poiché è possibile crittografare una copia di uno snapshot DB non crittografata, puoi aggiungere in modo efficace la crittografia a un'istanza database non crittografata. Ovvero, è possibile creare uno snapshot dell'istanza database e quindi creare una copia crittografata di quella snapshot. Puoi quindi ripristinare un'istanza database da uno snapshot crittografata e pertanto disporre di una copia crittografata dell'istanza database originale.

[RDS.5] Le istanze DB RDS devono essere configurate con più zone di disponibilità

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/2.2.4 NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 NIST.800-53.r5 SI-13 (5), Profilo CRI v2. 2/PR. IR-03.01

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : `rds-multi-az-support`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'alta disponibilità è abilitata per le istanze DB RDS. Il controllo fallisce se un'istanza DB RDS non è configurata con più zone di disponibilità (AZ). Questo controllo non si applica alle istanze DB RDS che fanno parte di una Multi-AZ distribuzione di cluster DB.

La configurazione delle istanze DB di Amazon RDS con AzS aiuta a garantire la disponibilità dei dati archiviati. Multi-AZ le implementazioni consentono il failover automatico in caso di problemi con la disponibilità di AZ e durante la normale manutenzione RDS.

Correzione

Per distribuire le tue istanze DB in più AZ, modifica di un'istanza DB per renderla una distribuzione di istanze Multi-AZ DB nella Amazon RDS User Guide.

[RDS.6] Il monitoraggio avanzato deve essere configurato per le istanze DB RDS

Requisiti correlati: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, CRI Profile v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. IR-04.01, Profilo CRI v2. 2/PR. PS-04.02

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : `rds-enhanced-monitoring-enabled`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`monitoringInterval`	Numero di secondi tra gli intervalli di raccolta delle metriche di monitoraggio	Enum	`1`, `5`, `10`, `15`, `30`, `60`	Nessun valore predefinito	

Questo controllo verifica se il monitoraggio avanzato è abilitato per un'istanza DB di Amazon Relational Database Service (Amazon RDS). Il controllo fallisce se il monitoraggio avanzato non è abilitato per l'istanza. Se fornisci un valore personalizzato per il `monitoringInterval` parametro, il controllo passa solo se le metriche di monitoraggio avanzate vengono raccolte per l'istanza all'intervallo specificato.

In Amazon RDS, Enhanced Monitoring consente una risposta più rapida ai cambiamenti delle prestazioni nell'infrastruttura sottostante. Queste modifiche delle prestazioni potrebbero comportare una mancanza di disponibilità dei dati. Enhanced Monitoring fornisce metriche in tempo reale del sistema operativo su cui viene eseguita l'istanza DB RDS. Sull'istanza è installato un agente. L'agente può ottenere le metriche in modo più accurato di quanto sia possibile dal livello dell'hypervisor.

I parametri di monitoraggio avanzato sono utili quando si desidera vedere come viene utilizzata la CPU in un'istanza database dai diversi processi o thread. Per ulteriori informazioni, consulta la sezione Enhanced Monitoring (Monitoraggio avanzato) nella Guida per l'utente di Amazon RDS.

Correzione

Per istruzioni dettagliate sull'attivazione di Enhanced Monitoring per la tua istanza DB, consulta Configurazione e attivazione di Enhanced Monitoring nella Amazon RDS User Guide.

[RDS.7] I cluster RDS devono avere la protezione da eliminazione abilitata

Requisiti correlati: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), CRI Profile v2. 2/PR. IR-03.01

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `rds-cluster-deletion-protection-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster RDS DB ha la protezione da eliminazione abilitata. Il controllo ha esito negativo se in un cluster RDS DB non è abilitata la protezione da eliminazione.

Questo controllo è destinato alle istanze DB RDS. Tuttavia, può anche generare risultati per le istanze Aurora DB, le istanze Neptune DB e i cluster Amazon DocumentDB. Se questi risultati non sono utili, puoi eliminarli.

L'attivazione della protezione dall'eliminazione del cluster è un ulteriore livello di protezione contro l'eliminazione accidentale del database o l'eliminazione da parte di un'entità non autorizzata.

Quando la protezione da eliminazione è abilitata, non è possibile eliminare un cluster RDS. Prima che una richiesta di eliminazione possa avere esito positivo, è necessario disabilitare la protezione dall'eliminazione.

Correzione

Per abilitare la protezione da eliminazione per un cluster RDS DB, consulta Modificare il cluster DB utilizzando la console, la CLI e l'API nella Amazon RDS User Guide. Per la protezione da eliminazione, scegli Abilita protezione da eliminazione.

[RDS.8] Le istanze DB RDS devono avere la protezione da eliminazione abilitata

Requisiti correlati: 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

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : `rds-instance-deletion-protection-enabled`

Tipo di pianificazione: modifica attivata

Parametri:

- `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` (non personalizzabile)

Questo controllo verifica se le istanze DB RDS che utilizzano uno dei motori di database elencati hanno la protezione dall'eliminazione abilitata. Il controllo ha esito negativo se per un'istanza RDS DB non è abilitata la protezione da eliminazione.

L'attivazione della protezione dall'eliminazione delle istanze è un ulteriore livello di protezione contro l'eliminazione accidentale del database o l'eliminazione da parte di un'entità non autorizzata.

Mentre la protezione dall'eliminazione è abilitata, un'istanza DB RDS non può essere eliminata. Prima che una richiesta di eliminazione possa avere esito positivo, è necessario disabilitare la protezione dall'eliminazione.

Correzione

Per abilitare la protezione da eliminazione per un'istanza DB RDS, consulta Modificare un'istanza DB Amazon RDS nella Amazon RDS User Guide. Per la protezione da eliminazione, scegli Abilita protezione da eliminazione.

[RDS.9] Le istanze DB RDS devono pubblicare i log in Logs CloudWatch

Requisiti correlati: 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), (4), NIST.800-53.r5 AU-6 (10) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8), PCI NIST.800-53.r5 SI-7 DSS v4.0. 1/10.2.1, Profilo CRI v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/PR. IR-04.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : `rds-logging-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istanza DB di Amazon RDS è configurata per pubblicare i seguenti log su Amazon CloudWatch Logs. Il controllo fallisce se l'istanza non è configurata per pubblicare i seguenti log su Logs: CloudWatch

- Oracle: Alert, Audit, Trace, Listener
- PostgreSQL: Postgresql, aggiornamento
- MySQL: controllo, errore, generale, SlowQuery
- MariaDB: controllo, errore, generale, SlowQuery
- SQL Server: errore, agente
- Aurora-MySQL: Controllo, Errore, Generale, SlowQuery
- Aurora-PostgreSQL: Postgresql

I database RDS devono avere i log pertinenti abilitati. La registrazione del database fornisce registrazioni dettagliate delle richieste effettuate a RDS. I log del database possono facilitare i controlli di sicurezza e accesso e possono aiutare a diagnosticare i problemi di disponibilità.

Correzione

Per informazioni sulla pubblicazione dei log del database RDS in CloudWatch Logs, consulta Specificare i log da pubblicare su Logs CloudWatch nella Amazon RDS User Guide.

[RDS.10] L'autenticazione IAM deve essere configurata per le istanze RDS

Requisiti correlati: 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 Profile v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-05.02, Profilo CRI v2. 2/PR. DS-01.01

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : `rds-instance-iam-authentication-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istanza DB RDS ha l'autenticazione del database IAM abilitata. Il controllo fallisce se l'autenticazione IAM non è configurata per le istanze DB RDS. Questo controllo valuta solo le istanze RDS con i seguenti tipi di motore:`mysql`,,,`postgres`, `aurora` e. `aurora-mysql` `aurora-postgresql` `mariadb` Un'istanza RDS deve inoltre trovarsi in uno dei seguenti stati per generare un risultato:`available`,, `backing-up` o. `storage-optimization` `storage-full`

L'autenticazione del database IAM consente l'autenticazione delle istanze del database con un token di autenticazione anziché una password. Il traffico di rete da e verso il database viene crittografato tramite SSL. Per ulteriori informazioni, consulta Autenticazione database IAM nella Guida per l'utente di Amazon Aurora.

Correzione

Per attivare l'autenticazione del database IAM su un'istanza DB RDS, consulta Abilitazione e disabilitazione dell'autenticazione del database IAM nella Amazon RDS User Guide.

[RDS.11] Le istanze RDS devono avere i backup automatici abilitati

Requisiti correlati: 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 SC-5 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13 (5) NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-11.01

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : `db-instance-backup-enabled`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`backupRetentionMinimum`	Periodo minimo di conservazione dei backup in giorni	Numero intero	Da 7 a 35	7	
`checkReadReplicas`	Verifica se le istanze DB RDS dispongono di backup abilitati per le repliche di lettura	Booleano	Non personalizzabile	`false`	

Questo controllo verifica se un'istanza di Amazon Relational Database Service ha abilitato i backup automatici e un periodo di conservazione dei backup maggiore o uguale al periodo di tempo specificato. Le repliche di lettura sono escluse dalla valutazione. Il controllo fallisce se i backup non sono abilitati per l'istanza o se il periodo di conservazione è inferiore al periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione del backup, Security Hub CSPM utilizza un valore predefinito di 7 giorni.

I backup consentono di ripristinare più rapidamente un incidente di sicurezza e rafforzano la resilienza dei sistemi. Amazon RDS consente di configurare istantanee giornaliere di volumi completi di istanze. Per ulteriori informazioni sui backup automatici di Amazon RDS, consulta Working with Backups nella Amazon RDS User Guide.

Correzione

Per abilitare i backup automatici su un'istanza DB RDS, consulta Enabling automation backup nella Amazon RDS User Guide.

[RDS.12] L'autenticazione IAM deve essere configurata per i cluster RDS

Requisiti correlati: 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 Profile v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-05.02, Profilo CRI v2. 2/PR. DS-01.01

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `rds-cluster-iam-authentication-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon RDS DB ha l'autenticazione del database IAM abilitata.

L'autenticazione del database IAM consente l'autenticazione senza password per le istanze di database. L'autenticazione utilizza un token di autenticazione. Il traffico di rete da e verso il database è crittografato tramite SSL. Per ulteriori informazioni, consulta Autenticazione database IAM nella Guida per l'utente di Amazon Aurora.

Correzione

Per abilitare l'autenticazione IAM per un cluster DB, consulta Abilitazione e disabilitazione dell'autenticazione del database IAM nella Guida per l'utente di Amazon Aurora.

[RDS.13] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/2.2.2, benchmark AWS CIS 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 versione 4.0. 1/6.3.3, Profilo CRI v2. 2/ID. RA-01.03, Profilo CRI v2. 2/PR. PS-02.01

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: alta

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : `rds-automatic-minor-version-upgrade-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se in un'istanza database Amazon RDS sono abilitati gli upgrade automatici delle versioni secondarie. Il controllo fallisce se gli aggiornamenti automatici delle versioni secondarie non sono abilitati per l'istanza DB RDS.

> **Note**
>
> Questo controllo valuta ogni istanza DB di Amazon RDS in modo indipendente. Per i cluster Amazon Aurora, gli aggiornamenti automatici delle versioni secondarie richiedono l'attivazione di questa impostazione sul cluster. È inoltre necessario abilitare questa impostazione su tutte le istanze del cluster. Un `PASSED` risultato per una singola istanza non garantisce che si verifichino aggiornamenti se non hai abilitato l'impostazione anche a livello di cluster.
> Inoltre, questo controllo non tiene conto delle configurazioni che non supportano gli aggiornamenti automatici delle versioni secondarie. Questi includono i cluster Aurora in un database globale Aurora e i cluster Aurora MySQL con repliche di lettura interregionali. Per queste configurazioni, il controllo potrebbe produrre risultati di valutazione che non riflettono accuratamente l'effettivo comportamento di aggiornamento.

Gli aggiornamenti automatici delle versioni secondarie aggiornano periodicamente un database alle versioni recenti del motore di database. Tuttavia, l'aggiornamento potrebbe non includere sempre la versione più recente del motore di database. Se è necessario mantenere i database su versioni specifiche in momenti particolari, consigliamo di eseguire manualmente l'aggiornamento alle versioni del database necessarie in base alla pianificazione richiesta. In caso di problemi di sicurezza critici

o quando una versione raggiunge la data di fine del supporto, Amazon RDS potrebbe applicare un aggiornamento della versione secondaria anche se non hai abilitato l'opzione Aggiornamento automatico della versione secondaria. Per ulteriori informazioni, consulta la documentazione di aggiornamento di Amazon RDS per il tuo motore di database specifico:

- Aggiornamenti automatici delle versioni secondarie per RDS per MariadB
- Aggiornamenti automatici delle versioni secondarie per RDS for MySQL
- Aggiornamenti automatici delle versioni secondarie per RDS per PostgreSQL
- Db2 nelle versioni di Amazon RDS
- Aggiornamenti delle versioni minori di Oracle
- Aggiornamenti del motore DB Microsoft SQL Server

Correzione

Per abilitare gli aggiornamenti automatici delle versioni secondarie per un'istanza DB esistente, consulta Modificare un'istanza DB Amazon RDS nella Amazon RDS User Guide. Per l'aggiornamento automatico delle versioni secondarie, seleziona Sì.

[RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato

Requisiti correlati: 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 SI-13 (5) NIST.800-53.r5 CP-9, CRI Profile v2. 2/GV. OC-05.04, Profilo CRI v2. 2/ID. IM-02.06, Profilo CRI v2. 2/PR. DS-11.01, Profilo CRI v2. 2/PR. IR-03.01

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `aurora-mysql-backtracking-enabled`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`BacktrackWindowInHours`	Numero di ore per il backtrack di un cluster Aurora MySQL	Double	Da `0.1` a `72`	Nessun valore predefinito	

Questo controllo verifica se un cluster Amazon Aurora ha il backtracking abilitato. Il controllo fallisce se il backtracking non è abilitato nel cluster. Se si fornisce un valore personalizzato per il `BacktrackWindowInHours` parametro, il controllo passa solo se il cluster viene eseguito a ritroso per il periodo di tempo specificato.

I backup consentono di ripristinare più rapidamente un incidente di sicurezza. Inoltre, rafforzano la resilienza dei sistemi. Il backtracking di Aurora riduce il tempo necessario per ripristinare un database a un determinato punto nel tempo. A tale scopo, non è necessario ripristinare il database.

Correzione

Per abilitare il backtracking di Aurora, consulta Configurazione del backtracking nella Guida per l'utente di Amazon Aurora.

Tieni presente che non puoi abilitare il backtracking su un cluster esistente. Puoi invece creare un clone con il backtracking abilitato. Per ulteriori informazioni sulle limitazioni del backtracking di Aurora, consulta l'elenco delle limitazioni in Panoramica del backtracking.

[RDS.15] I cluster RDS DB devono essere configurati per più zone di disponibilità

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/2.2.4 NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 NIST.800-53.r5 SI-13 (5), Profilo CRI v2. 2/PR. DS-11.01, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `rds-cluster-multi-az-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'alta disponibilità è abilitata per i cluster DB RDS. Il controllo fallisce se un cluster RDS DB non è distribuito in più zone di disponibilità (AZ).

I cluster RDS DB devono essere configurati per più AZ per garantire la disponibilità dei dati archiviati. L'implementazione su più AZ consente il failover automatico in caso di problemi di disponibilità AZ e durante i normali eventi di manutenzione RDS.

Correzione

Per distribuire i tuoi cluster DB in più AZ, modifica di un'istanza DB per renderla una distribuzione di istanze Multi-AZ DB nella Amazon RDS User Guide.

I passaggi di riparazione sono diversi per i database globali di Aurora. Per configurare più zone di disponibilità per un database globale Aurora, seleziona il tuo cluster DB. Quindi, scegli Azioni e Aggiungi lettore e specifica più AZ. Per ulteriori informazioni, consulta Aggiungere repliche Aurora a un cluster DB nella Amazon Aurora User Guide.

[RDS.16] I cluster Aurora DB devono essere configurati per copiare i tag nelle istantanee DB

Requisiti correlati: 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-08.01, Profilo CRI v2. 2/ID. AM-08.03

Categoria: Identificazione > Inventario

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBCluster`

AWS Config regola: `rds-cluster-copy-tags-to-snapshots-enabled` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Aurora DB è configurato per copiare automaticamente i tag negli snapshot del cluster DB al momento della creazione degli snapshot. Il controllo fallisce se il

cluster Aurora DB non è configurato per copiare automaticamente i tag nelle istantanee del cluster al momento della creazione delle istantanee.

L'identificazione e l'inventario delle risorse IT sono un aspetto cruciale della governance e della sicurezza. Devi avere la visibilità di tutti i tuoi cluster Amazon Aurora DB in modo da poterne valutare il livello di sicurezza e intervenire su potenziali aree di debolezza. Le istantanee di Aurora DB devono avere gli stessi tag dei cluster DB principali. In Amazon Aurora, puoi configurare un cluster DB per copiare automaticamente tutti i tag del cluster negli snapshot del cluster. L'attivazione di questa impostazione garantisce che gli snapshot DB ereditino gli stessi tag dei cluster DB principali.

Correzione

Per informazioni sulla configurazione di un cluster Amazon Aurora DB per copiare automaticamente i tag negli snapshot DB, consulta Modifying an Amazon Aurora DB cluster nella Amazon Aurora User Guide.

[RDS.17] Le istanze DB RDS devono essere configurate per copiare i tag negli snapshot

Requisiti correlati: 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-08.01, Profilo CRI v2. 2/ID. AM-08.03

Categoria: Identificazione > Inventario

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBInstance`

AWS Config regola: `rds-instance-copy-tags-to-snapshots-enabled` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le istanze DB RDS sono configurate per copiare tutti i tag nelle istantanee al momento della creazione delle istantanee.

L'identificazione e l'inventario delle risorse IT sono un aspetto cruciale della governance e della sicurezza. È necessario disporre della visibilità di tutte le istanze DB RDS in modo da poterne valutare il livello di sicurezza e intervenire sulle potenziali aree di debolezza. Le istantanee devono essere etichettate nello stesso modo delle istanze del database RDS principale. L'attivazione di questa impostazione garantisce che le istantanee ereditino i tag delle istanze di database principali.

Correzione

Per copiare automaticamente i tag negli snapshot per un'istanza DB RDS, consulta Modifying an Amazon RDS DB Instance nella Amazon RDS User Guide. Seleziona Copia i tag negli snapshot.

[RDS.19] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici del cluster

Requisiti correlati: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, CRI Profile v2. 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: `AWS::RDS::EventSubscription`

AWS Config regola: `rds-cluster-event-notifications-configured` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un abbonamento a eventi Amazon RDS esistente per cluster di database ha le notifiche abilitate per le seguenti coppie chiave-valore del tipo di origine e della categoria di evento:

```
DBCluster: ["maintenance","failure"]
```

Il controllo passa se non ci sono abbonamenti a eventi esistenti nel tuo account.

Le notifiche degli eventi RDS utilizzano Amazon SNS per informarti dei cambiamenti nella disponibilità o nella configurazione delle tue risorse RDS. Queste notifiche consentono una risposta rapida. Per ulteriori informazioni sulle notifiche degli eventi RDS, consulta Using Amazon RDS event notification nella Amazon RDS User Guide.

Correzione

Per iscriverti alle notifiche degli eventi del cluster RDS, consulta la sezione Sottoscrizione alla notifica degli eventi di Amazon RDS nella Amazon RDS User Guide. Utilizzare i seguenti valori:

Campo	Valore
Source type (Tipo di origine)	Cluster
Cluster da includere	Tutti i cluster
Categorie di eventi da includere	Seleziona categorie di eventi specifiche o Tutte le categorie di eventi

[RDS.20] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici delle istanze di database

Requisiti correlati: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115.2, Profilo CRI v2. 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: `AWS::RDS::EventSubscription`

AWS Config regola: `rds-instance-event-notifications-configured` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un abbonamento ad eventi Amazon RDS esistente per le istanze di database ha le notifiche abilitate per le seguenti coppie chiave-valore del tipo di origine e della categoria di evento:

```
DBInstance: ["maintenance","configuration change","failure"]
```

Il controllo passa se non ci sono abbonamenti a eventi esistenti nel tuo account.

Le notifiche degli eventi RDS utilizzano Amazon SNS per informarti dei cambiamenti nella disponibilità o nella configurazione delle tue risorse RDS. Queste notifiche consentono una risposta

rapida. Per ulteriori informazioni sulle notifiche degli eventi RDS, consulta Using Amazon RDS event notification nella Amazon RDS User Guide.

Correzione

Per iscriverti alle notifiche degli eventi delle istanze RDS, consulta la sezione Sottoscrizione alla notifica degli eventi di Amazon RDS nella Amazon RDS User Guide. Utilizzare i seguenti valori:

Campo	Valore
Source type (Tipo di origine)	Istanze
Istanze da includere	Tutte le istanze
Categorie di eventi da includere	Seleziona categorie di eventi specifiche o Tutte le categorie di eventi

[RDS.21] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database

Requisiti correlati: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115.2, Profilo CRI v2. 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: `AWS::RDS::EventSubscription`

AWS Config regola: `rds-pg-event-notifications-configured` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se esiste un abbonamento agli eventi Amazon RDS con le notifiche abilitate per le seguenti coppie chiave-valore del tipo di sorgente, categoria di evento. Il controllo passa se non ci sono abbonamenti a eventi esistenti nel tuo account.

```
DBParameterGroup: ["configuration change"]
```

Le notifiche degli eventi RDS utilizzano Amazon SNS per informarti dei cambiamenti nella disponibilità o nella configurazione delle tue risorse RDS. Queste notifiche consentono una risposta rapida. Per ulteriori informazioni sulle notifiche degli eventi RDS, consulta Using Amazon RDS event notification nella Amazon RDS User Guide.

Correzione

Per iscriverti alle notifiche degli eventi dei gruppi di parametri del database RDS, consulta la sezione Sottoscrizione alla notifica degli eventi di Amazon RDS nella Amazon RDS User Guide. Utilizzare i seguenti valori:

Campo	Valore
Source type (Tipo di origine)	Gruppi di parametri
Gruppi di parametri da includere	Tutti i gruppi di parametri
Categorie di eventi da includere	Seleziona categorie di eventi specifiche o Tutte le categorie di eventi

[RDS.22] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database

Requisiti correlati: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115.2, Profilo CRI v2. 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: `AWS::RDS::EventSubscription`

AWS Config regola: `rds-sg-event-notifications-configured` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se esiste un abbonamento agli eventi Amazon RDS con le notifiche abilitate per le seguenti coppie chiave-valore del tipo di sorgente, categoria di evento. Il controllo passa se non ci sono abbonamenti a eventi esistenti nel tuo account.

```
DBSecurityGroup: ["configuration change","failure"]
```

Le notifiche degli eventi RDS utilizzano Amazon SNS per informarti dei cambiamenti nella disponibilità o nella configurazione delle tue risorse RDS. Queste notifiche consentono una risposta rapida. Per ulteriori informazioni sulle notifiche degli eventi RDS, consulta Using Amazon RDS event notification nella Amazon RDS User Guide.

Correzione

Per iscriverti alle notifiche degli eventi delle istanze RDS, consulta la sezione Sottoscrizione alla notifica degli eventi di Amazon RDS nella Amazon RDS User Guide. Utilizzare i seguenti valori:

Campo	Valore
Source type (Tipo di origine)	Gruppi di sicurezza
Gruppi di sicurezza da includere	Tutti i gruppi di sicurezza
Categorie di eventi da includere	Seleziona categorie di eventi specifiche o Tutte le categorie di eventi

[RDS.23] Le istanze RDS non devono utilizzare una porta predefinita del motore di database

Requisiti correlati: 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 Profile v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03

Categoria: Protezione > Configurazione di rete protetta

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBInstance`

AWS Config regola: `rds-no-default-ports` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster o un'istanza RDS utilizza una porta diversa dalla porta predefinita del motore di database. Il controllo ha esito negativo se il cluster o l'istanza RDS utilizza la porta predefinita. Questo controllo non si applica alle istanze RDS che fanno parte di un cluster.

Se utilizzi una porta nota per distribuire un cluster o un'istanza RDS, un utente malintenzionato può indovinare le informazioni sul cluster o sull'istanza. L'autore dell'attacco può utilizzare queste informazioni insieme ad altre informazioni per connettersi a un cluster o a un'istanza RDS o ottenere informazioni aggiuntive sull'applicazione.

Quando si modifica la porta, è necessario aggiornare anche le stringhe di connessione esistenti utilizzate per connettersi alla porta precedente. È inoltre necessario controllare il gruppo di sicurezza dell'istanza DB per assicurarsi che includa una regola di ingresso che consenta la connettività sulla nuova porta.

Correzione

Per modificare la porta predefinita di un'istanza DB RDS esistente, consulta Modifying an Amazon RDS DB nella Amazon RDS User Guide. Per modificare la porta predefinita di un cluster RDS DB esistente, consulta Modificare il cluster DB utilizzando la console, la CLI e l'API nella Guida per l'utente di Amazon Aurora. Per la porta del database, modifica il valore della porta con un valore non predefinito.

[RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/2.2.2, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Identificazione > Configurazione delle risorse

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : `rds-cluster-default-admin-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster di database Amazon RDS ha modificato il nome utente dell'amministratore rispetto al valore predefinito. Il controllo non si applica ai motori del tipo neptune (Neptune DB) o docdb (DocumentDB). Questa regola avrà esito negativo se il nome utente dell'amministratore è impostato sul valore predefinito.

Quando crei un database Amazon RDS, devi modificare il nome utente amministratore predefinito con un valore univoco. I nomi utente predefiniti sono di dominio pubblico e devono essere modificati durante la creazione del database RDS. La modifica dei nomi utente predefiniti riduce il rischio di accessi involontari.

Correzione

Per modificare il nome utente di amministratore associato al cluster di database Amazon RDS, crea un nuovo cluster di database RDS e modifica il nome utente amministratore predefinito durante la creazione del database.

[RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/2.2.2, Profilo CRI v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Identificazione > Configurazione delle risorse

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : `rds-instance-default-admin-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se hai cambiato il nome utente amministrativo per le istanze di database Amazon Relational Database Service (Amazon RDS) rispetto al valore predefinito. Il controllo fallisce se il nome utente amministrativo è impostato sul valore predefinito. Il controllo non si applica ai motori del tipo neptune (Neptune DB) o docdb (DocumentDB) e alle istanze RDS che fanno parte di un cluster.

I nomi utente amministrativi predefiniti sui database Amazon RDS sono di dominio pubblico. Quando crei un database Amazon RDS, devi modificare il nome utente amministrativo predefinito con un valore univoco per ridurre il rischio di accessi involontari.

Correzione

Per modificare il nome utente amministrativo associato a un'istanza di database RDS, crea prima una nuova istanza di database RDS. Modifica il nome utente amministrativo predefinito durante la creazione del database.

[RDS.26] Le istanze DB RDS devono essere protette da un piano di backup

Categoria: Recover > Resilience > Backup abilitati

Requisiti correlati: 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 SC-5 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13 (5) NIST.800-53.r5 SI-12, CRI Profile v2. 2/PR. DS-11.01, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/RC. RP-01.01

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

AWS Config regola: **`rds-resources-protected-by-backup-plan`**

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`backupVaultLockCheck`	Il controllo produce un `PASSED` risultato se il parametro è impostato su true e la risorsa utilizza AWS Backup Vault Lock.	Booleano	`true` o `false`	Nessun valore predefinito	

Questo controllo valuta se le istanze database di Amazon RDS sono coperte da un piano di backup. Questo controllo fallisce se l'istanza DB RDS non è coperta da un piano di backup. Se si imposta il

`backupVaultLockCheck` parametro uguale `atrue`, il controllo passa solo se l'istanza è sottoposta a backup in un vault AWS Backup bloccato.

> **Note**
>
> Questo controllo non valuta le istanze di Neptune e DocumentDB. Inoltre, non valuta le istanze DB RDS che sono membri di un cluster.

AWS Backup è un servizio di backup completamente gestito che centralizza e automatizza il backup dei dati in tutto il mondo. Servizi AWS Con AWS Backup, è possibile creare politiche di backup denominate piani di backup. È possibile utilizzare questi piani per definire i requisiti di backup, ad esempio la frequenza con cui eseguire il backup dei dati e la durata di conservazione di tali backup. L'inclusione delle istanze DB RDS in un piano di backup consente di proteggere i dati da perdite o eliminazioni involontarie.

Correzione

Per aggiungere un'istanza DB RDS a un piano di AWS Backup backup, consulta Assegnazione di risorse a un piano di backup nella Guida per gli sviluppatori.AWS Backup

[RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi

Requisiti correlati: 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), (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

AWS Config regola: **`rds-cluster-encrypted-at-rest`**

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster DB RDS è crittografato quando è inattivo. Il controllo ha esito negativo se un cluster RDS DB non è crittografato a riposo.

I dati inattivi si riferiscono a tutti i dati archiviati in uno spazio di archiviazione persistente e non volatile per qualsiasi durata. La crittografia aiuta a proteggere la riservatezza di tali dati, riducendo il rischio che un utente non autorizzato possa accedervi. La crittografia dei cluster RDS DB protegge i dati e i metadati dall'accesso non autorizzato. Soddisfa inoltre i requisiti di conformità per la crittografia dei dati a riposo dei file system di produzione.

Correzione

È possibile abilitare la crittografia a riposo quando si crea un cluster RDS DB. Non è possibile modificare le impostazioni di crittografia dopo aver creato un cluster. Per ulteriori informazioni, consulta Encrypting an Amazon Aurora DB cluster nella Amazon Aurora User Guide.

[RDS.28] I cluster RDS DB devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBCluster`

AWS Config regola: `tagged-rds-dbcluster` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un cluster Amazon RDS DB dispone di tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il cluster DB non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro

`requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il cluster DB non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un cluster RDS DB, consulta Tagging delle risorse Amazon RDS nella Amazon RDS User Guide.

[RDS.29] Gli snapshot del cluster RDS DB devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBClusterSnapshot`

AWS Config regola: `tagged-rds-dbclustersnapshot` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se uno snapshot del cluster Amazon RDS DB contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se lo snapshot del cluster DB non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se lo snapshot del cluster DB non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a uno snapshot del cluster RDS DB, consulta Tagging delle risorse Amazon RDS nella Amazon RDS User Guide.

[RDS.30] Le istanze DB RDS devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBInstance`

AWS Config regola: `tagged-rds-dbinstance` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un'istanza database Amazon RDS dispone di tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se l'istanza DB non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e

fallisce se l'istanza DB non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'istanza DB RDS, consulta Tagging delle risorse Amazon RDS nella Amazon RDS User Guide.

[RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBSecurityGroup`

AWS Config regola: `tagged-rds-dbsecuritygroup` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un gruppo di sicurezza Amazon RDS DB dispone di tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il gruppo di sicurezza DB non dispone di chiavi di tag o se non dispone di tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di sicurezza DB non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gruppo di sicurezza RDS DB, consulta Tagging delle risorse Amazon RDS nella Amazon RDS User Guide.

[RDS.32] Gli snapshot RDS DB devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBSnapshot`

AWS Config regola: `tagged-rds-dbsnapshot` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se uno snapshot di Amazon RDS DB contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se lo snapshot DB non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se lo snapshot DB non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a uno snapshot DB RDS, consulta Tagging delle risorse Amazon RDS nella Amazon RDS User Guide.

[RDS.33] I gruppi di sottoreti RDS DB devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBSubnetGroup`

AWS Config regola: `tagged-rds-dbsubnetgroups` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un gruppo di sottoreti Amazon RDS DB dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gruppo di sottoreti DB non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di sottorete DB non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un sottogruppo di database RDS, consulta Tagging delle risorse Amazon RDS nella Amazon RDS User Guide.

[RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch

Requisiti correlati: 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), (20), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 PCI DSS NIST.800-53.r5 SI-7 v4.0. 1/10.2.1, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

AWS Config regola: **`rds-aurora-mysql-audit-logging-enabled`**

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Aurora MySQL DB è configurato per pubblicare log di audit su Amazon Logs. CloudWatch Il controllo fallisce se il cluster non è configurato per pubblicare i log di controllo su Logs. CloudWatch Il controllo non genera risultati per i cluster DB Aurora Serverless v1.

I log di controllo registrano le attività del database, inclusi tentativi di accesso, modifiche dei dati, modifiche dello schema e altri eventi che possono essere verificati per scopi di sicurezza e conformità. Quando configuri un cluster Aurora MySQL DB per pubblicare i log di controllo in un gruppo di log in Amazon CloudWatch Logs, puoi eseguire analisi in tempo reale dei dati di log. CloudWatch Logs conserva i log in uno storage altamente durevole. Puoi anche creare allarmi e visualizzare le metriche in. CloudWatch

> **Note**
>
> Un modo alternativo per pubblicare i log di controllo su CloudWatch Logs consiste nell'abilitare il controllo avanzato e impostare il parametro DB a livello di cluster su. `server_audit_logs_upload` `1` L'impostazione predefinita per è. `server_audit_logs_upload parameter` `0` Tuttavia, per passare questo controllo, si consiglia di utilizzare le seguenti istruzioni di riparazione.

Correzione

Per pubblicare i log di audit del cluster Aurora MySQL DB su Logs, CloudWatch consulta Pubblicazione dei log di Amazon Aurora MySQL su Amazon Logs nella Amazon Aurora User Guide. CloudWatch

[] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato

Requisiti correlati: 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. 1/6.3.3, Profilo CRI v2. 2/ID. RA-01.03, Profilo CRI v2. 2/PR. PS-02.01

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

AWS Config regola: **`rds-cluster-auto-minor-version-upgrade-enable`**

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'aggiornamento automatico della versione secondaria è abilitato per un cluster Amazon RDS DB, inclusi i cluster Aurora DB. Il controllo fallisce se l'aggiornamento automatico della versione secondaria non è abilitato per il cluster DB.

Con l'aggiornamento automatico della versione secondaria, puoi mantenere aggiornato il tuo cluster DB. Le versioni minori possono introdurre nuove funzionalità software, correzioni di bug, patch di sicurezza e miglioramenti delle prestazioni. Abilitando l'aggiornamento automatico delle

versioni secondarie sui cluster di database RDS, il cluster, insieme alle istanze del cluster, riceverà aggiornamenti automatici alla versione secondaria quando saranno disponibili nuove versioni. Gli aggiornamenti vengono applicati automaticamente durante la finestra di manutenzione.

Correzione

Per abilitare l'aggiornamento automatico delle versioni secondarie sui cluster Multi-AZ DB, consulta Modificare un cluster Multi-AZ DB nella Amazon RDS User Guide.

Per abilitare l'aggiornamento automatico delle versioni secondarie sui cluster Aurora DB, consulta Modificare un cluster Amazon Aurora DB nella Guida per l'utente di Amazon Aurora.

[RDS.36] Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch

Requisiti correlati: PCI DSS v4.0. 1/10.4.2, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : rds-postgresql-logs-to-cloudwatch

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`logTypes`	Comma-separated elenco dei tipi di log da pubblicare in Logs CloudWatch	StringList	Non personalizzabile	`postgresql`

Questo controllo verifica se un'istanza DB Amazon RDS for PostgreSQL è configurata per pubblicare log su Amazon Logs. CloudWatch Il controllo fallisce se l'istanza DB PostgreSQL non è configurata per pubblicare i tipi di log menzionati nel parametro su Logs. `logTypes` CloudWatch

La registrazione del database fornisce registrazioni dettagliate delle richieste effettuate a un'istanza RDS. PostgreSQL genera registri degli eventi che contengono informazioni utili per gli amministratori. La pubblicazione di questi log su CloudWatch Logs centralizza la gestione dei log e consente di eseguire analisi in tempo reale dei dati di registro. CloudWatch Logs conserva i log in uno spazio di archiviazione estremamente durevole. Puoi anche creare allarmi e visualizzare le metriche in. CloudWatch

Correzione

Per pubblicare i log delle istanze di PostgreSQL DB in Logs, consulta Pubblicazione dei log di PostgreSQL su Amazon CloudWatch Logs nella Amazon RDS User Guide. CloudWatch

[RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch

Requisiti correlati: PCI DSS v4.0. 1/10.4.2, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : rds-aurora-postgresql-logs-to-cloudwatch

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Aurora PostgreSQL DB è configurato per pubblicare log su Amazon Logs. CloudWatch Il controllo fallisce se il cluster Aurora PostgreSQL DB non è configurato per pubblicare i log PostgreSQL su Logs. CloudWatch

La registrazione del database fornisce registrazioni dettagliate delle richieste effettuate a un cluster RDS. Aurora PostgreSQL genera registri degli eventi che contengono informazioni utili per gli amministratori. La pubblicazione di questi log su Logs centralizza la gestione CloudWatch dei log e consente di eseguire analisi in tempo reale dei dati di registro. CloudWatch Logs conserva i log in uno spazio di archiviazione estremamente durevole. Puoi anche creare allarmi e visualizzare le metriche in. CloudWatch

Correzione

Per pubblicare i log del cluster Aurora PostgreSQL DB su Logs, consulta CloudWatch Pubblicazione dei log di Aurora PostgreSQL su Amazon Logs nella Amazon RDS User Guide. CloudWatch

[RDS.38] Le istanze DB RDS per PostgreSQL devono essere crittografate in transito

Requisiti correlati: CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : rds-postgres-instance-encrypted-in-transit

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se una connessione a un'istanza di Amazon RDS for PostgreSQL database (DB) è crittografata in transito. Il controllo ha esito negativo se il `rds.force_ssl` parametro per il gruppo di parametri associato all'istanza è impostato su `0` (off). Questo controllo non valuta le istanze DB RDS che fanno parte di un cluster DB.

I dati in transito si riferiscono ai dati che si spostano da una posizione all'altra, ad esempio tra i nodi del cluster o tra il cluster e l'applicazione. I dati possono spostarsi su Internet o all'interno di una rete privata. La crittografia dei dati in transito riduce il rischio che un utente non autorizzato possa intercettare il traffico di rete.

Correzione

Per richiedere che tutte le connessioni alla tua istanza DB RDS for PostgreSQL utilizzino SSL, consulta Using SSL with a PostgreSQL DB nella Amazon RDS User Guide.

[RDS.39] Le istanze DB RDS per MySQL devono essere crittografate in transito

Requisiti correlati: CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : rds-mysql-instance-encrypted-in-transit

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se una connessione a un'istanza di Amazon RDS for MySQL database (DB) è crittografata in transito. Il controllo ha esito negativo se il `rds.require_secure_transport` parametro per il gruppo di parametri associato all'istanza è impostato su `0` (off). Questo controllo non valuta le istanze DB RDS che fanno parte di un cluster DB.

I dati in transito si riferiscono ai dati che si spostano da una posizione all'altra, ad esempio tra i nodi del cluster o tra il cluster e l'applicazione. I dati possono spostarsi su Internet o all'interno di una rete privata. La crittografia dei dati in transito riduce il rischio che un utente non autorizzato possa intercettare il traffico di rete.

Correzione

Per richiedere che tutte le connessioni alla tua istanza DB RDS for MySQL utilizzino SSL, consulta il SSL/TLS supporto per le istanze DB MySQL su Amazon RDS nella Amazon RDS User Guide.

[RDS.40] Le istanze DB di RDS per SQL Server devono pubblicare i log in Logs CloudWatch

Requisiti correlati: 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 SC-7 (10) NIST.800-53.r5 CA-7, (9), 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

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : rds-sql-server-logs-to-cloudwatch

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`logTypes`	Un elenco dei tipi di log che un'istanza DB di RDS per SQL Server deve essere configurata per pubblicare nei registri. CloudWatch Questo controllo ha esito negativo se un'istanza DB non è configura ta per pubblicare un tipo di log specificato nell'elenco.	EnumList (massimo 2 elementi)	`agent`, `error`	`agent`, `error`

Questo controllo verifica se un'istanza DB di Amazon RDS for Microsoft SQL Server è configurata per pubblicare log su Amazon CloudWatch Logs. Il controllo fallisce se l'istanza DB RDS per SQL Server non è configurata per pubblicare log su Logs. CloudWatch Facoltativamente, è possibile specificare i tipi di log che un'istanza DB deve essere configurata per la pubblicazione.

La registrazione del database fornisce record dettagliati delle richieste effettuate a un'istanza database Amazon RDS. La pubblicazione dei log su CloudWatch Logs centralizza la gestione dei log e consente di eseguire analisi in tempo reale dei dati di log. CloudWatch Logs conserva i log in uno spazio di archiviazione altamente durevole. Inoltre, è possibile utilizzarlo per creare allarmi per errori specifici che possono verificarsi, ad esempio riavvii frequenti registrati in un registro degli errori. Allo stesso modo, è possibile creare allarmi per errori o avvisi registrati nei registri degli agenti di SQL Server relativi ai processi di SQL Agent.

Correzione

Per informazioni sulla pubblicazione dei log in CloudWatch Logs per un'istanza DB RDS for SQL Server, consulta i file di log del database Amazon RDS for Microsoft SQL Server nella Amazon Relational Database Service User Guide.

[RDS.41] Le istanze DB di RDS per SQL Server devono essere crittografate in transito

Requisiti correlati: CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : rds-sqlserver-encrypted-in-transit

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se una connessione a un'istanza DB di Amazon RDS for Microsoft SQL Server è crittografata in transito. Il controllo fallisce se il `rds.force_ssl` parametro del gruppo di parametri associato all'istanza DB è impostato `0 (off)` su.

I dati in transito si riferiscono ai dati che si spostano da una posizione all'altra, ad esempio tra i nodi di un cluster DB o tra un cluster DB e un'applicazione client. I dati possono spostarsi su Internet o all'interno di una rete privata. La crittografia dei dati in transito riduce il rischio che utenti non autorizzati intercettino il traffico di rete.

Correzione

Per informazioni sull'abilitazione SSL/TLS delle connessioni alle istanze DB di Amazon RDS che eseguono Microsoft SQL Server, consulta Using SSL with a Microsoft SQL Server DB nella Amazon Relational Database Service User Guide.

[RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch

Requisiti correlati: 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, (9) NIST.800-53.r5 AU-12 NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (10), 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

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : mariadb-publish-logs-to-cloudwatch-logs

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`logTypes`	Un elenco dei tipi di log che un'istanza DB MariaDB deve essere configurata per pubblicare su Logs. CloudWatch Il controllo genera un `FAILED` risultato se un'istanza DB non è configura ta per pubblicare un tipo di log specificato nell'elenco.	EnumList (massimo 4 elementi)	`audit`, `error`, `general`, `slowquery`	`audit, error`

Questo controllo verifica se un'istanza Amazon RDS for MariaDB DB è configurata per pubblicare determinati tipi di log su Amazon Logs. CloudWatch Il controllo fallisce se l'istanza di MariaDB DB non è configurata per pubblicare i log su Logs. CloudWatch Puoi facoltativamente specificare quali tipi di log deve essere configurata per la pubblicazione di un'istanza DB MariaDB.

La registrazione del database fornisce record dettagliati delle richieste effettuate a un'istanza Amazon RDS for MariaDB DB. La pubblicazione dei log su Amazon CloudWatch Logs centralizza la gestione dei log e consente di eseguire analisi in tempo reale dei dati di log. Inoltre, CloudWatch Logs conserva i log in uno storage durevole, che può supportare revisioni e verifiche di sicurezza, accesso e disponibilità. Con CloudWatch Logs, puoi anche creare allarmi e rivedere le metriche.

Correzione

Per informazioni sulla configurazione di un'istanza Amazon RDS for MariaDB DB per pubblicare i log su Amazon Logs, consulta Pubblicazione dei log di MariaDB CloudWatch su Amazon Logs nella Amazon CloudWatch Relational Database Service User Guide.

[] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::RDS::DBProxy`

Regola AWS Config : rds-proxy-tls-encryption

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un proxy Amazon RDS DB richiede TLS per tutte le connessioni tra il proxy e l'istanza database RDS sottostante. Il controllo fallisce se il proxy non richiede TLS per tutte le connessioni tra il proxy e l'istanza DB RDS.

Amazon RDS Proxy può fungere da ulteriore livello di sicurezza tra le applicazioni client e le istanze DB RDS sottostanti. Ad esempio, puoi connetterti a un proxy RDS utilizzando TLS 1.3, anche se l'istanza DB sottostante supporta una versione precedente di TLS. Utilizzando RDS Proxy, è possibile applicare requisiti di autenticazione rigorosi per le applicazioni di database.

Correzione

Per informazioni sulla modifica delle impostazioni affinché un proxy Amazon RDS richieda TLS, consulta Modifying an RDS proxy nella Amazon Relational Database Service User Guide.

[RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito

Requisiti correlati: CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06, Profilo CRI v2. 2/PR. PS-06.10

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : rds-mariadb-instance-encrypted-in-transit

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se le connessioni a un'istanza Amazon RDS for MariaDB DB sono crittografate in transito. Il controllo fallisce se il gruppo di parametri DB associato all'istanza DB non è sincronizzato o il `require_secure_transport` parametro del gruppo di parametri non è impostato su. `ON`

> **Note**
>
> Questo controllo non valuta le istanze DB di Amazon RDS che utilizzano versioni di MariaDB precedenti alla versione 10.5. Il `require_secure_transport` parametro è supportato solo per le versioni MariadB 10.5 e successive.

I dati in transito si riferiscono ai dati che si spostano da una posizione all'altra, ad esempio tra i nodi di un cluster DB o tra un cluster DB e un'applicazione client. I dati possono spostarsi su Internet o all'interno di una rete privata. La crittografia dei dati in transito riduce il rischio che utenti non autorizzati intercettino il traffico di rete.

Correzione

Per informazioni sull'abilitazione SSL/TLS delle connessioni a un'istanza Amazon RDS for MariaDB DB, SSL/TLS consulta la sezione Richiesta di tutte le connessioni a un'istanza DB MariaDB nella Amazon Relational Database Service User Guide.

[RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata

Requisiti correlati: 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-6 (3) NIST.800-53.r5 AU-3, (4),,, NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12 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 CRI Profile NIST.800-53.r5 SI-7 v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : aurora-mysql-cluster-audit-logging

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Aurora MySQL DB ha la registrazione di controllo abilitata. Il controllo fallisce se il gruppo di parametri DB associato al cluster DB non è sincronizzato, il

`server_audit_logging` parametro non è impostato su o il `server_audit_events` parametro è impostato su un valore vuoto. 1

I log del database possono facilitare i controlli di sicurezza e accesso e aiutare a diagnosticare i problemi di disponibilità. I registri di controllo registrano le attività del database, inclusi i tentativi di accesso, le modifiche dei dati, le modifiche allo schema e altri eventi che possono essere verificati per scopi di sicurezza e conformità.

Correzione

Per informazioni sull'abilitazione della registrazione per un cluster Amazon Aurora MySQL DB, consulta Pubblicazione dei log di Amazon Aurora MySQL su Amazon Logs nella Amazon Aurora User Guide. CloudWatch

[RDS.46] Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso gateway Internet

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::RDS::DBInstance`

Regola AWS Config : rds-instance-subnet-igw-check

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un'istanza database Amazon RDS è distribuita in una sottorete pubblica con un percorso verso un gateway Internet. Il controllo ha esito negativo se l'istanza DB RDS viene distribuita in una sottorete con un percorso verso un gateway Internet e la destinazione è impostata su o. `0.0.0.0/0 ::/0`

Effettuando il provisioning delle risorse Amazon RDS in sottoreti private, puoi impedire alle risorse RDS di ricevere traffico in entrata dalla rete Internet pubblica, impedendo così l'accesso involontario alle tue istanze DB RDS. Se le risorse RDS vengono fornite in una sottorete pubblica aperta a Internet, potrebbero essere vulnerabili a rischi come l'esfiltrazione dei dati.

Correzione

Per informazioni sul provisioning di una sottorete privata per un'istanza DB Amazon RDS, consulta Working with a DB istance in a VPC nella Amazon Relational Database Service User Guide.

[RDS.47] I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : rds-pgsql-cluster-copy-tags-to-snapshot-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon RDS for PostgreSQL DB è configurato per copiare automaticamente i tag negli snapshot del cluster DB al momento della creazione degli snapshot. Il controllo ha esito negativo se il `CopyTagsToSnapshot` parametro è impostato su `false` per il cluster DB RDS for PostgreSQL.

La copia dei tag nelle istantanee del DB aiuta a mantenere il monitoraggio delle risorse, la governance e l'allocazione dei costi corretti tra le risorse di backup. Ciò consente l'identificazione coerente delle risorse, il controllo degli accessi e il monitoraggio della conformità sia nei database attivi che nelle relative istantanee. Le istantanee con tag appropriati migliorano le operazioni di sicurezza assicurando che le risorse di backup ereditino gli stessi metadati dei database di origine.

Correzione

Per informazioni sulla configurazione di un cluster Amazon RDS for PostgreSQL DB per copiare automaticamente i tag negli snapshot DB, consulta Tagging Amazon RDS resources nella Amazon Relational Database Service User Guide.

[RDS.48] I cluster RDS per MySQL DB devono essere configurati per copiare i tag nelle istantanee del DB

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : rds-mysql-cluster-copy-tags-to-snapshot-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon RDS for MySQL DB è configurato per copiare automaticamente i tag negli snapshot del cluster DB al momento della creazione degli snapshot. Il controllo ha esito negativo se il `CopyTagsToSnapshot` parametro è impostato su `false` per il cluster DB RDS for MySQL.

La copia dei tag nelle istantanee del DB aiuta a mantenere il monitoraggio delle risorse, la governance e l'allocazione dei costi corretti tra le risorse di backup. Ciò consente l'identificazione coerente delle risorse, il controllo degli accessi e il monitoraggio della conformità sia nei database attivi che nelle relative istantanee. Le istantanee con tag appropriati migliorano le operazioni di sicurezza assicurando che le risorse di backup ereditino gli stessi metadati dei database di origine.

Correzione

Per informazioni sulla configurazione di un cluster Amazon RDS for MySQL DB per copiare automaticamente i tag negli snapshot DB, consulta Tagging Amazon RDS resources nella Amazon Relational Database Service User Guide.

[RDS.50] I cluster RDS DB devono avere un periodo di conservazione dei backup sufficiente

Categoria: Recover > Resilience > Backup abilitati

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : rds-cluster-backup-retention-check

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`minimumBackupReten`	Periodo minimo di conservazione del backup, espresso in	Numero intero	Da 7 a 35	7	

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`tionPeriod`	giorni, per la verifica del controllo				

Questo controllo verifica se un cluster RDS DB ha un periodo minimo di conservazione dei backup. Il controllo ha esito negativo se il periodo di conservazione del backup è inferiore al valore del parametro specificato. A meno che non si fornisca un valore di parametro personalizzato, Security Hub utilizza un valore predefinito di 7 giorni.

Questo controllo verifica se un cluster RDS DB ha un periodo minimo di conservazione dei backup. Il controllo ha esito negativo se il periodo di conservazione del backup è inferiore al valore del parametro specificato. A meno che non si fornisca un valore del parametro cliente, Security Hub utilizza un valore predefinito di 7 giorni. Questo controllo si applica a tutti i tipi di cluster RDS DB, inclusi il cluster Aurora DB, i cluster DocumentDB, i cluster NeptuneDB, ecc.

Correzione

Per configurare il periodo di conservazione dei backup per un cluster RDS DB, modifica le impostazioni del cluster e imposta il periodo di conservazione del backup su almeno 7 giorni (o il valore specificato nel parametro di controllo). Per istruzioni dettagliate, consulta il periodo di conservazione del backup nella Guida per l'utente di Amazon Relational Database Service. Per i cluster Aurora DB, consulta Panoramica del backup e del ripristino di un cluster Aurora DB nella Guida per l'utente di Amazon Aurora per Aurora. Per altri tipi di cluster DB (ad esempio cluster DocumentDB), consulta la guida per l'utente del servizio corrispondente su come aggiornare il periodo di conservazione dei backup per il cluster.

[RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: alta

Tipo di risorsa: `AWS::RDS::GlobalCluster`

Regola AWS Config : rds-global-cluster-aurora-mysql-supported-version

Tipo di pianificazione: modifica attivata

Parametri:

- `minSupportedEngineVersion`: `8.0.mysql_aurora.3.08.0` (non personalizzabile)
- `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` (non personalizzabile)

Questo controllo verifica se un cluster globale Amazon Aurora MySQL è in esecuzione su una versione minima del motore supportata. Il controllo fallisce se la versione del motore di cluster globale Aurora MySQL è inferiore alla versione minima supportata specificata e non è elencata nel parametro della versione di supporto a lungo termine.

L'esecuzione dei database globali Aurora MySQL su versioni del motore supportate aiuta a garantire l'accesso alle ultime patch di sicurezza, correzioni di bug e miglioramenti delle prestazioni. Le versioni secondarie di Aurora MySQL hanno date di fine supporto standard definite, dopo le quali non ricevono più patch critiche. L'esecuzione di una versione non supportata può esporre il database globale a vulnerabilità di sicurezza e può comportare costi di Amazon RDS Extended Support. Poiché Aurora MySQL segue un ciclo di vita del supporto non contiguo in cui le versioni LTS (Long-Term Support) rimangono supportate più a lungo rispetto alle successive versioni non LTS, questo controllo verifica anche le versioni LTS che rientrano ancora nel supporto standard. Per ulteriori informazioni, consulta i calendari di rilascio per Amazon Aurora MySQL nelle note di rilascio di Amazon Aurora per Aurora MySQL.

Correzione

Per informazioni sull'aggiornamento di un database globale Aurora MySQL a una versione del motore supportata, consulta Aggiornamento di un database globale Amazon Aurora e Aggiornamento di Aurora MySQL modificando la versione del motore nella Guida per l'utente di Amazon Aurora.

Controlli CSPM del Security Hub per Amazon Redshift

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon Redshift. I controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico

Requisiti correlati: 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. 1/1.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 1/1.3.6, PCI DSS versione 4.0. 1/1.4.4, Profilo CRI v2. 2/PR. IR-01.01

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Severità: critica

Tipo di risorsa: `AWS::Redshift::Cluster`

Regola AWS Config : redshift-cluster-public-access-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i cluster Amazon Redshift sono accessibili pubblicamente. Valuta il `PubliclyAccessible` campo nell'elemento di configurazione del cluster.

L'`PubliclyAccessible`attributo della configurazione del cluster Amazon Redshift indica se il cluster è accessibile pubblicamente. Quando il cluster è configurato con `PubliclyAccessible` set to`true`, si tratta di un' Internet-facing istanza con un nome DNS risolvibile pubblicamente, che si risolve in un indirizzo IP pubblico.

Quando il cluster non è accessibile pubblicamente, si tratta di un'istanza interna con un nome DNS che si risolve in un indirizzo IP privato. A meno che non si intenda rendere il cluster accessibile pubblicamente, il cluster non deve essere configurato con `PubliclyAccessible` set to. `true`

Correzione

Per aggiornare un cluster Amazon Redshift per disabilitare l'accesso pubblico, consulta Modifying a cluster nella Amazon Redshift Management Guide. Imposta l'accesso pubblico su No.

[Redshift.2] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito

Requisiti correlati: 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. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

Regola AWS Config : redshift-require-tls-ssl

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le connessioni ai cluster Amazon Redshift sono necessarie per utilizzare la crittografia in transito. Il controllo ha esito negativo se il parametro del cluster Amazon Redshift `require_SSL` non è impostato su. `True`

Il TLS può essere usato per impedire a potenziali aggressori di utilizzare attacchi person-in-the-middle o attacchi simili per intercettare o manipolare il traffico di rete. Dovrebbero essere consentite solo le connessioni crittografate tramite TLS. La crittografia dei dati in transito può influire sulle prestazioni. È consigliabile testare l'applicazione con questa funzionalità per comprendere il profilo delle prestazioni e l'impatto del TLS.

Correzione

Per aggiornare un gruppo di parametri Amazon Redshift per richiedere la crittografia, consulta Modificare un gruppo di parametri nella Amazon Redshift Management Guide. Impostato su **`require_ssl`** True.

[Redshift.3] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate

Requisiti correlati: 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 (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-13 (5), CRI Profile v2. 2/PR. DS-11.01

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: `AWS::Redshift::Cluster`

Regola AWS Config : redshift-backup-enabled

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub	
`MinRetentionPeriod`	Periodo minimo di conservazione delle istantanee in giorni	Numero intero	Da 7 a 35	7	

Questo controllo verifica se un cluster Amazon Redshift ha abilitato le istantanee automatiche e un periodo di conservazione maggiore o uguale al periodo di tempo specificato. Il controllo fallisce se le istantanee automatiche non sono abilitate per il cluster o se il periodo di conservazione è inferiore al periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione delle istantanee, Security Hub CSPM utilizza un valore predefinito di 7 giorni.

I backup consentono di ripristinare più rapidamente un incidente di sicurezza. Rafforzano la resilienza dei sistemi. Amazon Redshift acquisisce istantanee periodiche per impostazione predefinita. Questo controllo verifica se le istantanee automatiche sono abilitate e conservate per almeno sette giorni. Per ulteriori dettagli sugli snapshot automatizzati di Amazon Redshift, consulta Snapshot automatizzati nella Amazon Redshift Management Guide.

Correzione

Per aggiornare il periodo di conservazione degli snapshot per un cluster Amazon Redshift, consulta Modifying a cluster nella Amazon Redshift Management Guide. Per Backup, imposta la conservazione delle istantanee su un valore pari o superiore a 7.

[Redshift.4] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata

Requisiti correlati: 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. 1/10.2.1, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::Redshift::Cluster`

AWS Config regola: `redshift-cluster-audit-logging-enabled` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Redshift ha abilitato la registrazione di audit.

La registrazione di controllo di Amazon Redshift fornisce informazioni aggiuntive sulle connessioni e sulle attività degli utenti nel cluster. Questi dati possono essere archiviati e protetti in Amazon S3 e possono essere utili per controlli e indagini di sicurezza. Per ulteriori informazioni, consulta Database audit logging nella Amazon Redshift Management Guide.

Correzione

Per configurare la registrazione di audit per un cluster Amazon Redshift, consulta Configurazione del controllo con la console nella Amazon Redshift Management Guide.

[Redshift.6] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati

Requisiti correlati: 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 (2) NIST.800-53.r5 SI-2, (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), CRI Profile v2. 2/PR. PS-02.01, Profilo CRI v2. 2/PR. PS-02.03

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: `AWS::Redshift::Cluster`

Regola AWS Config : redshift-cluster-maintenancesettings-check

Tipo di pianificazione: modifica attivata

Parametri:

- `allowVersionUpgrade = true`(non personalizzabile)

Questo controllo verifica se gli upgrade automatici delle versioni principali sono abilitati per il cluster Amazon Redshift.

L'abilitazione degli aggiornamenti automatici delle versioni principali garantisce che gli ultimi aggiornamenti delle versioni principali dei cluster Amazon Redshift vengano installati durante la finestra di manutenzione. Questi aggiornamenti potrebbero includere patch di sicurezza e correzioni di bug. Mantenersi aggiornati sull'installazione delle patch è un passaggio importante per proteggere i sistemi.

Correzione

Per risolvere questo problema da AWS CLI, usa il comando Amazon `modify-cluster` Redshift e imposta `--allow-version-upgrade` l'attributo. *`clustername`*è il nome del tuo cluster Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

[Redshift.7] I cluster Redshift devono utilizzare un routing VPC avanzato

Requisiti correlati: 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), (20), 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 (9), CRI Profile v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.03

Categoria: Protezione > Configurazione di rete sicura > Accesso privato alle API

Gravità: media

Tipo di risorsa: `AWS::Redshift::Cluster`

Regola AWS Config : redshift-enhanced-vpc-routing-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Redshift è `EnhancedVpcRouting` abilitato.

Il routing VPC migliorato impone a tutto il `UNLOAD` traffico tra il cluster `COPY` e gli archivi di dati di passare attraverso il tuo VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare VPC Flow Logs per monitorare il traffico di rete.

Correzione

Per istruzioni dettagliate sulla riparazione, consulta Enhancing Enhanced VPC routing nella Amazon Redshift Management Guide.

[Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/PR. AA-01.01

Categoria: Identificazione > Configurazione delle risorse

Gravità: media

Tipo di risorsa: `AWS::Redshift::Cluster`

Regola AWS Config : redshift-default-admin-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Redshift ha modificato il nome utente dell'amministratore rispetto al valore predefinito. Questo controllo avrà esito negativo se il nome utente di amministratore per un cluster Redshift è impostato su. `awsuser`

Quando si crea un cluster Redshift, è necessario modificare il nome utente amministratore predefinito con un valore univoco. I nomi utente predefiniti sono di dominio pubblico e devono essere modificati al momento della configurazione. La modifica dei nomi utente predefiniti riduce il rischio di accessi involontari.

Correzione

Non puoi modificare il nome utente di amministratore per il tuo cluster Amazon Redshift dopo averlo creato. Per creare un nuovo cluster con un nome utente non predefinito, consulta la Fase 1: Creare un cluster Amazon Redshift di esempio nella Amazon Redshift Getting Started Guide.

[Redshift.10] I cluster Redshift devono essere crittografati a riposo

Requisiti correlati: 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, NIST.800-53.r5 SI-7 (6), CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::Redshift::Cluster`

Regola AWS Config : redshift-cluster-kms-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i cluster Amazon Redshift sono crittografati quando sono inattivi. Il controllo fallisce se un cluster Redshift non è crittografato a riposo o se la chiave di crittografia è diversa dalla chiave fornita nel parametro della regola.

In Amazon Redshift è possibile attivare la crittografia del database per i cluster per proteggere ulteriormente i dati a riposo. Quando si attiva la crittografia per un cluster, i blocchi di dati e i metadati di sistema vengono crittografati per il cluster e i relativi snapshot. La crittografia dei dati inattivi è una best practice consigliata perché aggiunge un livello di gestione degli accessi ai dati. La crittografia dei cluster Redshift a riposo riduce il rischio che un utente non autorizzato possa accedere ai dati archiviati su disco.

Correzione

Per modificare un cluster Redshift per utilizzare la crittografia KMS, consulta Changing cluster encryption nella Amazon Redshift Management Guide.

[Redshift.11] I cluster Redshift devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Redshift::Cluster`

AWS Config regola: `tagged-redshift-cluster` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un cluster Amazon Redshift dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il cluster non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un cluster Redshift, consulta Tagging resources in Amazon Redshift nella Amazon Redshift Management Guide.

[Redshift.12] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Redshift::EventSubscription`

AWS Config regola: `tagged-redshift-eventsubscription` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se uno snapshot del cluster Amazon Redshift contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se lo snapshot del cluster non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una

chiave di tag e fallisce se lo snapshot del cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un abbonamento di notifica di eventi Redshift, consulta Tagging resources in Amazon Redshift nella Amazon Redshift Management Guide.

[Redshift.13] Le istantanee del cluster Redshift devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Redshift::ClusterSnapshot`

AWS Config regola: `tagged-redshift-clustersnapshot` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se uno snapshot del cluster Amazon Redshift contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se lo snapshot del cluster non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se lo snapshot del cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a uno snapshot del cluster Redshift, consulta Tagging resources in Amazon Redshift nella Amazon Redshift Management Guide.

[Redshift.14] I gruppi di sottoreti del cluster Redshift devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Redshift::ClusterSubnetGroup`

AWS Config regola: `tagged-redshift-clustersubnetgroup` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un sottogruppo di cluster Amazon Redshift ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gruppo di sottoreti del cluster non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di sottorete del cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un sottogruppo di cluster Redshift, consulta Tagging resources in Amazon Redshift nella Amazon Redshift Management Guide.

[Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate

Requisiti correlati: PCI DSS v4.0. 1/1.3.1, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. DS-01.02, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.02

Categoria: Protezione > Configurazione di rete sicura > Configurazione del gruppo di sicurezza

Gravità: alta

Tipo di risorsa: `AWS::Redshift::Cluster`

Regola AWS Config : redshift-unrestricted-port-access

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un gruppo di sicurezza associato a un cluster Amazon Redshift ha regole di ingresso che consentono l'accesso alla porta del cluster da Internet (0.0.0. 0/0 o: :/0). Il controllo fallisce se le regole di ingresso del gruppo di sicurezza consentono l'accesso alla porta del cluster da Internet.

Consentire l'accesso in entrata senza restrizioni alla porta del cluster Redshift (indirizzo IP con suffisso /0) può causare accessi non autorizzati o incidenti di sicurezza. Si consiglia di applicare il principio dell'accesso con privilegi minimi durante la creazione di gruppi di sicurezza e la configurazione delle regole in entrata.

Correzione

Per limitare l'ingresso sulla porta del cluster Redshift a origini limitate, consulta Work with security group rules nella Amazon VPC User Guide. Aggiorna le regole in cui l'intervallo di porte corrisponde alla porta del cluster Redshift e l'intervallo di porte IP è 0.0.0. 0/0.

[Redshift.16] I gruppi di sottoreti del cluster Redshift devono avere sottoreti provenienti da più zone di disponibilità

Requisiti correlati: CRI Profile v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::Redshift::ClusterSubnetGroup`

Regola AWS Config : redshift-cluster-subnet-group-multi-az

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Il controllo verifica se un gruppo di sottoreti del cluster Amazon Redshift ha sottoreti provenienti da più di una zona di disponibilità (AZ). Il controllo fallisce se il gruppo di sottoreti del cluster non dispone di sottoreti provenienti da almeno due AZ diverse.

La configurazione delle sottoreti su più AZ aiuta a garantire che il data warehouse Redshift possa continuare a funzionare anche quando si verificano eventi di errore.

Correzione

Per modificare un sottogruppo di cluster Redshift in modo che si estenda su più AZ, consulta Modificare un gruppo di sottoreti del cluster nella Amazon Redshift Management Guide.

[Redshift.17] I gruppi di parametri del cluster Redshift devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Redshift::ClusterParameterGroup`

Regola AWS Config : redshift-cluster-parameter-group-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un gruppo di parametri del cluster Amazon Redshift ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo fallisce se il gruppo di parametri non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di parametri non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta creata e assegnata a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare,

organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un gruppo di parametri del cluster Amazon Redshift, consulta Tag resources in Amazon Redshift nella Amazon Redshift Management Guide.

[Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ

Requisiti correlati: CRI Profile v2. 2/GV. OC-04.03, Profilo CRI v2. 2/GV. RM-09.02, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::Redshift::Cluster`

Regola AWS Config : redshift-cluster-multi-az-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le distribuzioni di più zone di disponibilità (Multi-AZ) sono abilitate per un cluster Amazon Redshift. Il controllo fallisce se Multi-AZ le distribuzioni non sono abilitate per il cluster Amazon Redshift.

Amazon Redshift supporta implementazioni di più zone di disponibilità (Multi-AZ) per cluster con provisioning. Se Multi-AZ le implementazioni sono abilitate per un cluster, un data warehouse

Amazon Redshift può continuare a funzionare in scenari di errore quando si verifica un evento imprevisto in una zona di disponibilità (AZ). Una Multi-AZ distribuzione distribuisce risorse di elaborazione in più di una zona di disponibilità e a tali risorse di calcolo è possibile accedervi tramite un singolo endpoint. In caso di guasto dell'intera zona AZ, le risorse di elaborazione rimanenti in un'altra zona sono disponibili per continuare a elaborare i carichi di lavoro. È possibile convertire un Single-AZ data warehouse esistente in un Multi-AZ data warehouse. Le risorse di elaborazione aggiuntive vengono quindi fornite in una seconda zona di disponibilità.

Correzione

Per informazioni sulla configurazione delle Multi-AZ distribuzioni per un cluster Amazon Redshift, consulta Convertire un Single-AZ data warehouse in un data warehouse Multi-AZ nella Amazon Redshift Management Guide.

Controlli CSPM del Security Hub per Amazon Redshift Serverless

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon Redshift Serverless. I controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato

Requisiti correlati: CRI Profile v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-06.10

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Gravità: alta

Tipo di risorsa: `AWS::RedshiftServerless::Workgroup`

Regola AWS Config : redshift-serverless-workgroup-routes-within-vpc

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se il routing VPC avanzato è abilitato per un gruppo di lavoro Amazon Redshift Serverless. Il controllo fallisce se il routing VPC avanzato è disabilitato per il gruppo di lavoro.

Se il routing VPC avanzato è disabilitato per un gruppo di lavoro Amazon Redshift Serverless, Amazon Redshift indirizza il traffico attraverso Internet, incluso il traffico verso altri servizi all'interno della rete. AWS Se abiliti il routing VPC avanzato per un gruppo di lavoro, Amazon Redshift impone tutto il `UNLOAD` traffico tra il cluster `COPY` e i tuoi repository di dati attraverso il tuo cloud privato virtuale (VPC) basato sul servizio Amazon VPC. Con il routing VPC migliorato, puoi utilizzare le funzionalità VPC standard per controllare il flusso di dati tra il cluster Amazon Redshift e altre risorse. Ciò include funzionalità come i gruppi di sicurezza VPC e le politiche degli endpoint, le liste di controllo degli accessi alla rete (ACL) e i server Domain Name System (DNS). Puoi anche utilizzare i log di flusso in VPC per monitorare `COPY` il traffico. `UNLOAD`

Correzione

Per ulteriori informazioni sul routing VPC avanzato e su come abilitarlo per un gruppo di lavoro, consulta Controlling network traffic with Redshift Enhanced VPC routing nella Amazon Redshift Management Guide.

[RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL

Requisiti correlati: CRI Profile v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::RedshiftServerless::Workgroup`

Regola AWS Config : redshift-serverless-workgroup-encrypted-in-transit

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se le connessioni a un gruppo di lavoro Serverless Amazon Redshift sono necessarie per crittografare i dati in transito. Il controllo fallisce se il parametro di `require_ssl` configurazione per il gruppo di lavoro è impostato su. `false`

Un gruppo di lavoro Serverless Amazon Redshift è una raccolta di risorse di elaborazione che raggruppa risorse di calcolo come RPU, sottogruppi di sottoreti VPC e gruppi di sicurezza. Le proprietà di un gruppo di lavoro includono impostazioni di rete e sicurezza. Queste impostazioni

specificano se devono essere necessarie le connessioni a un gruppo di lavoro per utilizzare SSL per crittografare i dati in transito.

Correzione

Per informazioni sull'aggiornamento delle impostazioni per un gruppo di lavoro Amazon Redshift Serverless per richiedere connessioni SSL, consulta Connecting to Amazon Redshift Serverless nella Amazon Redshift Management Guide.

[RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico

Requisiti correlati: CRI Profile v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. DS-01.02, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::RedshiftServerless::Workgroup`

Regola AWS Config : redshift-serverless-workgroup-no-public-access

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se l'accesso pubblico è disabilitato per un gruppo di lavoro Serverless Amazon Redshift. Valuta la `publiclyAccessible` proprietà di un gruppo di lavoro Redshift Serverless. Il controllo fallisce se l'accesso pubblico è abilitato (`true`) per il gruppo di lavoro.

L'impostazione public access (`publiclyAccessible`) per un gruppo di lavoro Amazon Redshift Serverless specifica se è possibile accedere al gruppo di lavoro da una rete pubblica. Se l'accesso pubblico è abilitato (`true`) per un gruppo di lavoro, Amazon Redshift crea un indirizzo IP elastico che rende il gruppo di lavoro accessibile pubblicamente dall'esterno del VPC. Se non vuoi che un gruppo di lavoro sia accessibile al pubblico, disabilita l'accesso pubblico per esso.

Correzione

Per informazioni sulla modifica dell'impostazione di accesso pubblico per un gruppo di lavoro Serverless Amazon Redshift, consulta Visualizzazione delle proprietà di un gruppo di lavoro nella Amazon Redshift Management Guide.

[RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys

Requisiti correlati: 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),, (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

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::RedshiftServerless::Namespace`

Regola AWS Config : redshift-serverless-namespace-cmk-encryption

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`kmsKeyArns`	Un elenco di Amazon Resource Names (ARN) AWS KMS keys da includere nella valutazione. Il controllo genera un `FAILED` risultato se uno spazio dei nomi Redshift Serverless non è crittografato con una chiave KMS nell'elenco.	StringList (massimo 3 articoli)	1—3 ARN di chiavi KMS esistenti. Ad esempio: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` .	Nessun valore predefinito

Questo controllo verifica se uno spazio dei nomi Amazon Redshift Serverless è crittografato quando è inattivo e gestito dal cliente. AWS KMS key Il controllo fallisce se lo spazio dei nomi Redshift Serverless non è crittografato con una chiave KMS gestita dal cliente. Facoltativamente, puoi specificare un elenco di chiavi KMS per il controllo da includere nella valutazione.

In Amazon Redshift Serverless, uno spazio dei nomi definisce un container logico per gli oggetti del database. Questo controllo verifica periodicamente se le impostazioni di crittografia per un namespace specificano una chiave KMS gestita dal cliente AWS KMS key, anziché una chiave KMS AWS gestita, per la crittografia dei dati nello spazio dei nomi. Con una chiave KMS gestita dal cliente, hai il pieno controllo della chiave. Ciò include la definizione e il mantenimento della politica chiave, la gestione delle sovvenzioni, la rotazione del materiale crittografico, l'assegnazione di tag, la creazione di alias e l'attivazione e la disabilitazione della chiave.

Correzione

Per informazioni sull'aggiornamento delle impostazioni di crittografia per uno spazio dei nomi Amazon Redshift Serverless e sulla specificazione di un namespace gestito dal cliente AWS KMS key, consulta Changing the AWS KMS key for a namespace nella Amazon Redshift Management Guide.

[RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito

Categoria: Identificazione > Configurazione delle risorse

Gravità: media

Tipo di risorsa: `AWS::RedshiftServerless::Namespace`

Regola AWS Config : redshift-serverless-default-admin-check

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se il nome utente di amministratore per uno spazio dei nomi Amazon Redshift Serverless è il nome utente amministratore predefinito,. `admin` Il controllo fallisce se il nome utente di amministratore per lo spazio dei nomi Redshift Serverless è. `admin`

Quando crei uno spazio dei nomi Amazon Redshift Serverless, devi specificare un nome utente amministratore personalizzato per lo spazio dei nomi. Il nome utente amministratore predefinito è di

dominio pubblico. Specificando un nome utente di amministratore personalizzato, puoi, ad esempio, contribuire a mitigare il rischio o l'efficacia degli attacchi di forza bruta contro il namespace.

Correzione

Puoi modificare il nome utente di amministratore per uno spazio dei nomi Amazon Redshift Serverless utilizzando la console o l'API Amazon Redshift Serverless. Per modificarlo utilizzando la console, scegli la configurazione dello spazio dei nomi, quindi scegli Modifica credenziali di amministratore nel menu Azioni. Per modificarla a livello di codice, usa l'UpdateNamespaceoperazione o, se usi il, esegui il AWS CLI comando update-namespace. Se modifichi il nome utente dell'amministratore, devi modificare contemporaneamente anche la password dell'amministratore.

[RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch

Requisiti correlati: CRI Profile v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::RedshiftServerless::Namespace`

Regola AWS Config : redshift-serverless-publish-logs-to-cloudwatch

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se uno spazio dei nomi Amazon Redshift Serverless è configurato per esportare i log di connessione e utente in Amazon Logs. CloudWatch Il controllo fallisce se lo spazio dei nomi Redshift Serverless non è configurato per esportare i log in Logs. CloudWatch

Se configuri Amazon Redshift Serverless per esportare i dati di log di connessione (`connectionlog`) e log degli utenti (`userlog`) in un gruppo di log in Amazon CloudWatch Logs, puoi raccogliere e archiviare i tuoi record di log in uno storage durevole, che può supportare revisioni e verifiche di sicurezza, accesso e disponibilità. Con CloudWatch Logs, puoi anche eseguire analisi in tempo reale dei dati di log e utilizzarli CloudWatch per creare allarmi e rivedere i parametri.

Correzione

Per esportare i dati di log per uno spazio dei nomi Amazon Redshift Serverless in CloudWatch Amazon Logs, è necessario selezionare i rispettivi log per l'esportazione nelle impostazioni di configurazione di audit logging per lo spazio dei nomi. Per informazioni sull'aggiornamento di queste impostazioni, consulta Modifica della sicurezza e della crittografia nella Amazon Redshift Management Guide.

Controlli CSPM del Security Hub per Route 53

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse di Amazon Route 53.

Questi controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Route53.1] I controlli sanitari della Route 53 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Route53::HealthCheck`

AWS Config regola: `tagged-route53-healthcheck` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un controllo dello stato di Amazon Route 53 contiene tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il controllo dello stato non contiene alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il controllo di integrità non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un controllo di integrità della Route 53, consulta i controlli di integrità di denominazione e etichettatura nella Amazon Route 53 Developer Guide.

[Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS

Requisiti correlati: 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. 1/10.4.2, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::Route53::HostedZone`

Regola AWS Config : `route53-query-logging-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione delle query DNS è abilitata per una zona ospitata pubblica di Amazon Route 53. Il controllo fallisce se la registrazione delle query DNS non è abilitata per una zona ospitata pubblicamente su Route 53.

La registrazione delle query DNS per una zona ospitata su Route 53 soddisfa i requisiti di sicurezza e conformità DNS e garantisce la visibilità. I log includono informazioni quali il dominio o il sottodominio su cui è stata eseguita la query, la data e l'ora della query, il tipo di record DNS (ad esempio, A o AAAA) e il codice di risposta DNS (ad esempio o). `NoError` `ServFail` Quando la registrazione delle query DNS è abilitata, Route 53 pubblica i file di registro su Amazon Logs. CloudWatch

Correzione

Per registrare le query DNS per le zone ospitate pubbliche di Route 53, consulta Configurazione della registrazione per le query DNS nella Amazon Route 53 Developer Guide.

Controlli CSPM del Security Hub per Amazon S3

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon Simple Storage Service (Amazon S3). I controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/2.1.4, benchmark AWS CIS Foundations v3.0. 0/2.1.4, benchmark AWS CIS 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), (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 NIST.800-53.r5

SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS versione 3.2. 1/1.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 1/1.3.6, PCI DSS versione 4.0. 1/1.4.4, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. IR-01.01

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : s3-account-level-public-access-blocks-periodic

Tipo di pianificazione: periodica

Parametri:

- `ignorePublicAcls`: `true` (non personalizzabile)
- `blockPublicPolicy`: `true` (non personalizzabile)
- `blockPublicAcls`: `true` (non personalizzabile)
- `restrictPublicBuckets`: `true` (non personalizzabile)

Questo controllo verifica se le precedenti impostazioni di accesso pubblico a blocchi di Amazon S3 sono configurate a livello di account per un bucket S3 generico. Il controllo fallisce se una o più impostazioni di accesso pubblico a blocchi sono impostate su. `false`

Il controllo ha esito negativo se una delle impostazioni è impostata su o se una delle impostazioni non è configurata. `false`

Il blocco di accesso pubblico di Amazon S3 è progettato per fornire controlli su un intero bucket S3 Account AWS o a livello di singolo bucket S3 per garantire che gli oggetti non abbiano mai accesso pubblico. L'accesso pubblico viene concesso a bucket e oggetti tramite liste di controllo accessi (ACL), policy di bucket o entrambi.

A meno che tu non intenda rendere i tuoi bucket S3 accessibili al pubblico, devi configurare la funzionalità Amazon S3 Block Public Access a livello di account.

Per ulteriori informazioni, consulta Using Amazon S3 Block Public Access nella Guida per l'utente di Amazon Simple Storage Service.

Correzione

Per abilitare Amazon S3 Block Public Access per il tuo account Account AWS, consulta Configurazione delle impostazioni di accesso pubblico a blocchi per il tuo account nella Guida per l'utente di Amazon Simple Storage Service.

[S3.2] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura

Requisiti correlati: PCI DSS v3.2. 1/12.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 1/1.3.6, PCI DSS versione 3.2. 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), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. IR-01.01

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-bucket-public-read-prohibited

Tipo di pianificazione: periodica e con attivazione di modifiche

Parametri: nessuno

Questo controllo verifica se un bucket Amazon S3 per uso generico consente l'accesso pubblico in lettura. Esamina le impostazioni di blocco dell'accesso pubblico, la policy del bucket e la lista di controllo accessi (ACL) del bucket. Il controllo fallisce se il bucket consente l'accesso pubblico in lettura.

> **Note**
>
> Se un bucket S3 ha una policy bucket, questo controllo non valuta le condizioni delle policy che utilizzano caratteri jolly o variabili. Per produrre un `PASSED` risultato, le condizioni della bucket policy devono utilizzare solo valori fissi, ossia valori che non contengono caratteri jolly o variabili di policy. Per informazioni sulle variabili di policy, consulta Variabili e tag nella Guida per l'AWS Identity and Access Management utente.

Alcuni casi d'uso potrebbero richiedere che tutti gli utenti di Internet siano in grado di leggere dal tuo bucket S3. Tuttavia, queste situazioni sono rare. Per garantire l'integrità e la sicurezza dei dati, il bucket S3 non deve essere leggibile pubblicamente.

Correzione

Per bloccare l'accesso pubblico in lettura sui tuoi bucket Amazon S3, consulta Configurazione delle impostazioni di accesso pubblico a blocchi per i tuoi bucket S3 nella Guida per l'utente di Amazon Simple Storage Service.

[S3.3] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura

Requisiti correlati: PCI DSS v3.2. 1/12.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 1/1.3.6, PCI DSS versione 3.2. 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), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. IR-01.01

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-bucket-public-write-prohibited

Tipo di pianificazione: periodica e con attivazione di modifiche

Parametri: nessuno

Questo controllo verifica se un bucket Amazon S3 per uso generico consente l'accesso pubblico in scrittura. Esamina le impostazioni di blocco dell'accesso pubblico, la policy del bucket e la lista di controllo accessi (ACL) del bucket. Il controllo fallisce se il bucket consente l'accesso pubblico in scrittura.

> **Note**
>
> Se un bucket S3 ha una policy bucket, questo controllo non valuta le condizioni delle policy che utilizzano caratteri jolly o variabili. Per produrre un `PASSED` risultato, le condizioni della

bucket policy devono utilizzare solo valori fissi, ossia valori che non contengono caratteri jolly o variabili di policy. Per informazioni sulle variabili di policy, consulta Variabili e tag nella Guida per l'AWS Identity and Access Management utente.

Alcuni casi d'uso prevedono che chiunque su Internet sia in grado di scrivere nel bucket S3. Tuttavia, queste situazioni sono rare. Per garantire l'integrità e la sicurezza dei dati, il bucket S3 non deve essere scrivibile pubblicamente.

Correzione

Per bloccare l'accesso pubblico in scrittura sui tuoi bucket Amazon S3, consulta Configurazione delle impostazioni di accesso pubblico a blocchi per i tuoi bucket S3 nella Guida per l'utente di Amazon Simple Storage Service.

[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/2.1.1, benchmark AWS CIS Foundations v3.0. 0/2.1.1, benchmark AWS CIS 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), (1), NIST.800-53.r5 SC-7 (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 versione 3.2. NIST.800-171.r2 1/4.1, PCI DSS versione 4.0. 1/4.2.1, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-bucket-ssl-requests-only

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un bucket Amazon S3 per uso generico ha una politica che richiede richieste di utilizzo di TLS. Il controllo fallisce se la policy del bucket non richiede richieste di utilizzo di TLS.

I bucket S3 devono avere politiche che richiedono che tutte le richieste (`Action: S3:*`) accettino solo la trasmissione di dati tramite HTTPS nella politica delle risorse S3, indicata dalla chiave di condizione. `aws:SecureTransport`

Correzione

Per aggiornare una policy sui bucket di Amazon S3 per impedire il trasporto non sicuro, consulta Aggiungere una policy sui bucket utilizzando la console Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Aggiungi una dichiarazione di policy simile a quella riportata nella seguente policy. Sostituiscilo `amzn-s3-demo-bucket` con il nome del bucket che stai modificando.

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": "*"
        }
    ]
}
```

Per ulteriori informazioni, consulta Quale policy sui bucket S3 devo usare per rispettare la regola s3-bucket-ssl-requests-only? AWS Config nel Knowledge Center ufficiale.AWS

[S3.6] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-171.r2 3.13.4 NIST.800-53.r5 CM-2, CRI Profile v2. 2/PR. AA-05.01

Categoria: Protezione > Gestione sicura degli accessi > Azioni operative API sensibili limitate

Gravità: alta

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config: s3-bucket-blacklisted-actions-prohibited

Tipo di pianificazione: modifica attivata

Parametri:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl` (non personalizzabile)

Questo controllo verifica se una policy sui bucket generici di Amazon S3 impedisce ai principali di eseguire azioni negate sulle risorse nel bucket S3. Account AWS Il controllo fallisce se la bucket policy consente una o più delle azioni precedenti per un principale in un altro. Account AWS

L'implementazione dell'accesso con privilegi minimi è fondamentale per ridurre i rischi per la sicurezza e l'impatto di errori o intenzioni malevole. Se una policy S3 bucket consente l'accesso da account esterni, potrebbe causare l'esfiltrazione dei dati da parte di una minaccia interna o di un aggressore.

Il `blacklistedactionpatterns` parametro consente una valutazione corretta della regola per i bucket S3. Il parametro consente l'accesso agli account esterni per i modelli di azione che non sono inclusi nell'elenco. `blacklistedactionpatterns`

Correzione

Per aggiornare una policy sui bucket di Amazon S3 per rimuovere le autorizzazioni, consulta. Aggiungere una policy bucket utilizzando la console Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Nella pagina Modifica policy bucket, nella casella di testo per la modifica della policy, esegui una delle seguenti azioni:

- Rimuovi le dichiarazioni che concedono ad altri Account AWS l'accesso alle azioni negate.
- Rimuovi le azioni negate consentite dalle dichiarazioni.

[S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni

Requisiti correlati: 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 NIST.800-53.r5 SI-13 (5), profilo CRI v2. 2/GV. OC-05.03, Profilo CRI v2. 2/GV. OC-05.04, Profilo CRI v2. 2/PR. DS-11.01, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. IR-04.02, Profilo CRI v2. 2/RC. RP-03.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: `AWS::S3::Bucket`

AWS Config regola: s3-bucket-cross-region-replication-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se in un bucket Amazon S3 per uso generico è abilitata la replica tra regioni. Il controllo fallisce se nel bucket non è abilitata la replica tra regioni.

La replica è la copia automatica e asincrona di oggetti tra bucket uguali o diversi. Regioni AWS La replica copia gli oggetti appena creati e gli aggiornamenti degli oggetti da un bucket di origine a uno o più bucket di destinazione. AWS le migliori pratiche consigliano la replica per i bucket di origine e di destinazione di proprietà degli stessi. Account AWS Oltre alla disponibilità, è necessario prendere in considerazione altre impostazioni di protezione dei sistemi.

Questo controllo produce una `FAILED` ricerca per un bucket di destinazione di replica se non ha la replica tra regioni abilitata. Se esiste un motivo legittimo per cui il bucket di destinazione non necessita della replica tra regioni per essere abilitato, puoi sopprimere i risultati per questo bucket.

Correzione

Per abilitare Cross-Region la replica su un bucket S3, consulta Configurazione della replica per i bucket di origine e destinazione di proprietà dello stesso account nella Amazon Simple Storage Service User Guide. Per Source bucket, scegli Applica a tutti gli oggetti nel bucket.

[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/2.1.4, benchmark AWS CIS Foundations v3.0.02.1.4, benchmark CIS Foundations v1.4. AWS 0/2.1.5, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, 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 (9), NIST.800-53.r5 SC-7 PCI DSS versione 4.0 NIST.800-53.r5 SC-7. NIST.800-53.r5 SC-7 1/1.4.4, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.03, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Gravità: alta

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-bucket-level-public-access-prohibited

Tipo di pianificazione: modifica attivata

Parametri:

- `excludedPublicBuckets`(non personalizzabile): un elenco separato da virgole di nomi di bucket S3 pubblici e noti e consentiti

Questo controllo verifica se un bucket generico Amazon S3 blocca l'accesso pubblico a livello di bucket. Il controllo fallisce se una delle seguenti impostazioni è impostata su: `false`

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

Block Public Access a livello di bucket S3 fornisce controlli per garantire che gli oggetti non abbiano mai accesso pubblico. L'accesso pubblico viene concesso a bucket e oggetti tramite liste di controllo accessi (ACL), policy di bucket o entrambi.

A meno che tu non intenda rendere i tuoi bucket S3 accessibili al pubblico, devi configurare la funzionalità Amazon S3 Block Public Access a livello di bucket.

Correzione

Per informazioni su come rimuovere l'accesso pubblico a livello di bucket, consulta Bloccare l'accesso pubblico allo storage Amazon S3 nella Amazon S3 User Guide.

[S3.9] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata

Requisiti correlati: 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.800-171.r2 3.3.8, NIST.800-53.r5 SI-7 PCI DSS v4.0. 1/10.2.1, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/PR. PS-04.02

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-bucket-logging-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione degli accessi al server è abilitata per un bucket Amazon S3 per uso generico. Il controllo fallisce se la registrazione degli accessi al server non è abilitata. Quando la registrazione è abilitata, Amazon S3 fornisce i log di accesso per un bucket di origine a un bucket di destinazione scelto. Il bucket di destinazione deve trovarsi nello stesso Regione AWS del bucket di origine e non deve avere un periodo di conservazione predefinito configurato. Non è necessario che nel bucket di registrazione di destinazione sia abilitata la registrazione degli accessi al server ed è necessario eliminare i risultati relativi a questo bucket.

La registrazione degli accessi al server fornisce registrazioni dettagliate delle richieste effettuate a un bucket. I log di accesso al server possono aiutare nei controlli di sicurezza e di accesso. Per ulteriori informazioni, consulta Best practice di sicurezza per Amazon S3: abilitare la registrazione degli accessi ai server Amazon S3.

Correzione

Per abilitare la registrazione degli accessi ai server Amazon S3, consulta Enabling Amazon S3 server access logging nella Amazon S3 User Guide.

[S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita

Requisiti correlati: 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), CRI Profile v2. 2/ID. AM-08.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-version-lifecycle-policy-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un bucket con versione generica di Amazon S3 ha una configurazione del ciclo di vita. Il controllo fallisce se il bucket non ha una configurazione del ciclo di vita.

Ti consigliamo di creare una configurazione del ciclo di vita per il tuo bucket S3 per aiutarti a definire le azioni che desideri che Amazon S3 intraprenda durante la vita di un oggetto.

> **Tip**
>
> L'abilitazione del controllo delle versioni senza la gestione del ciclo di vita può portare a una crescita illimitata dello storage e a un aumento dei costi. Ogni modifica dell'oggetto crea una nuova versione che viene conservata a tempo indeterminato. Configura le regole del ciclo di vita di S3 per trasferire automaticamente le versioni non correnti a classi di storage più economiche o farle scadere dopo un periodo di conservazione definito.

Correzione

Per ulteriori informazioni sulla configurazione del ciclo di vita su un bucket Amazon S3, consulta Using S3 Versioning with S3 Lifecycle, Setting lifecycle configuration on a bucket e Managing the lifecycle of objects nella Amazon S3 User Guide.

[] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate

Requisiti correlati: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (4) NIST.800-53.r5 SI-4, NIST.800-171.r2 3.3.8, CRI Profile v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. PS-04.01, Profilo CRI v2. 2/PR. PS-04.02

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-event-notifications-enabled

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`eventTypes`	Elenco dei tipi di eventi S3 preferiti	EnumList (massimo 28 articoli)	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`, `s3:LifecycleExpiration:DeleteMarkerCreated`, `s3:Lifecy`	Nessun valore predefinito

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
			cleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMarkerCreated,	

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
			s3:ObjectRestore:*, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication,	

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
			`s3:Replication:OperationMissedThreshold`, `s3:Replication:OperationNotTracked`, `s3:Replication:OperationReplicatedAfterThreshold`, `s3:TestEvent`	

Questo controllo verifica se le notifiche degli eventi S3 sono abilitate su un bucket Amazon S3 per uso generico. Il controllo fallisce se le notifiche degli eventi S3 non sono abilitate nel bucket. Se fornisci valori personalizzati per il `eventTypes` parametro, il controllo passa solo se le notifiche degli eventi sono abilitate per i tipi di eventi specificati.

Quando abiliti le notifiche di eventi S3, ricevi avvisi quando si verificano eventi specifici che influiscono sui bucket S3. Ad esempio, puoi ricevere notifiche sulla creazione, la rimozione e il ripristino degli oggetti. Queste notifiche possono avvisare i team competenti in caso di modifiche accidentali o intenzionali che possono portare all'accesso non autorizzato ai dati.

Correzione

Per informazioni sul rilevamento delle modifiche ai bucket e agli oggetti S3, consulta Amazon S3 Event Notifications nella Amazon S3 User Guide.

[S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3

Requisiti correlati: 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 Profile v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Gravità: media

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-bucket-acl-prohibited

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un bucket Amazon S3 per uso generico fornisce autorizzazioni utente con una lista di controllo degli accessi (ACL). Il controllo fallisce se un ACL è configurato per la gestione dell'accesso degli utenti al bucket.

Gli ACL sono meccanismi di controllo degli accessi legacy precedenti a IAM. Invece degli ACL, consigliamo di utilizzare le policy dei bucket S3 o le policy AWS Identity and Access Management (IAM) per gestire l'accesso ai bucket S3.

Correzione

Per passare questo controllo, devi disabilitare gli ACL per i tuoi bucket S3. Per istruzioni, consulta Controllare la proprietà degli oggetti e disabilitare gli ACL per il tuo bucket nella Guida per l'utente di Amazon Simple Storage Service.

Per creare una policy per i bucket S3, consulta Aggiungere una policy per i bucket utilizzando la console Amazon S3. Per creare una policy utente IAM su un bucket S3, consulta Controllare l'accesso a un bucket con le policy utente.

[S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita

Requisiti correlati: 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), CRI Profile v2. 2/ID. AM-08.01

Categoria: Proteggi > Protezione dei dati

Gravità: bassa

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-lifecycle-policy-check

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`targetTransitionDays`	Numero di giorni dopo la creazione dell'oggetto, quando gli oggetti vengono trasferiti a una classe di archiviazione specificata	Numero intero	Da `1` a `36500`	Nessun valore predefinito
`targetExpirationDays`	Numero di giorni dopo la creazione dell'oggetto in cui gli oggetti vengono eliminati	Numero intero	Da `1` a `36500`	Nessun valore predefinito
`targetTransitionStorageClass`	Tipo di classe di archiviazione S3 di destinazione	Enum	`STANDARD_IA`, `INTELLIGENT_TIERING`, `ONEZONE_IA`, `GLACIER`, `GLACIER_IR`, `DEEP_ARCHIVE`	Nessun valore predefinito

Questo controllo verifica se un bucket Amazon S3 per uso generico ha una configurazione del ciclo di vita. Il controllo fallisce se il bucket non ha una configurazione del ciclo di vita. Se fornisci valori personalizzati per uno o più dei parametri precedenti, il controllo passa solo se la policy include la classe di archiviazione, il tempo di eliminazione o il tempo di transizione specificati.

La creazione di una configurazione del ciclo di vita per il tuo bucket S3 definisce le azioni che vuoi che Amazon S3 intraprenda durante la vita di un oggetto. Ad esempio, puoi trasferire oggetti in un'altra classe di storage, archiviarli o eliminarli dopo un periodo di tempo specificato.

Correzione

Per informazioni sulla configurazione delle politiche del ciclo di vita su un bucket Amazon S3, consulta Setting lifecycle configuration on a bucket e Managing your storage lifecycle nella Amazon S3 User Guide.

S3.14[] I bucket S3 per uso generico devono avere il controllo delle versioni abilitato

Categoria: Proteggi > Protezione dei dati > Protezione dalla cancellazione dei dati

Requisiti correlati: 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), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13 (5) NIST.800-53.r5 SI-12, NIST.800-171.r2 3.3.8, CRI Profile v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. IR-03.01, Profilo CRI v2. 2/PR. PS-01.03

Gravità: bassa

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-bucket-versioning-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un bucket Amazon S3 per uso generico ha il controllo delle versioni abilitato. Il controllo fallisce se il controllo delle versioni è sospeso per il bucket.

Il controllo delle versioni mantiene più varianti di un oggetto nello stesso bucket S3. Puoi utilizzare il controllo delle versioni per conservare, recuperare e ripristinare tutte le versioni di tutti gli oggetti archiviati nel tuo bucket S3. Il controllo delle versioni ti aiuta a recuperare sia da azioni involontarie dell'utente che da errori delle applicazioni.

> **Tip**
>
> L'abilitazione del controllo delle versioni senza la gestione del ciclo di vita può portare a una crescita illimitata dello storage e a un aumento dei costi. Ogni modifica dell'oggetto crea una nuova versione che viene conservata a tempo indeterminato. Configura le regole del ciclo di vita di S3 per trasferire automaticamente le versioni non correnti a classi di storage più economiche o farle scadere dopo un periodo di conservazione definito. Per ulteriori informazioni, consulta Utilizzo del controllo delle versioni di S3 con S3 Lifecycle e Gestione del ciclo di vita degli oggetti.

Correzione

Per utilizzare il controllo delle versioni su un bucket S3, consulta Enabling versioning on bucket nella Amazon S3 User Guide.

[S3.15] I bucket generici S3 devono avere Object Lock abilitato

Categoria: Proteggi > Protezione dei dati > Protezione dalla cancellazione dei dati

Requisiti correlati: NIST.800-53.r5 CP-6 (2), PCI DSS v4.0. 1/10.5.1, Profilo CRI v2. 2/DE. CM-09.01, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/PR. DS-11.01

Gravità: media

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-bucket-default-lock-enabled

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`mode`	Modalità di conservazione di S3 Object Lock	Enum	`GOVERNANCE` ,	Nessun valore predefinito

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
			`COMPLIANCE`	

Questo controllo verifica se un bucket Amazon S3 per uso generico ha Object Lock abilitato. Il controllo fallisce se Object Lock non è abilitato per il bucket. Se fornite un valore personalizzato per il `mode` parametro, il controllo passa solo se S3 Object Lock utilizza la modalità di conservazione specificata.

Puoi utilizzare il blocco oggetti S3 per archiviare gli oggetti utilizzando il modello write-once-read-many (WORM). Object Lock può aiutare a impedire che gli oggetti nei bucket S3 vengano eliminati o sovrascritti per un periodo di tempo fisso o indefinitamente. Puoi utilizzare il blocco oggetti S3 per soddisfare i requisiti normativi che richiedono uno storage WORM o aggiungere un ulteriore livello di protezione contro le modifiche e l'eliminazione degli oggetti.

Correzione

Per configurare Object Lock per bucket S3 nuovi ed esistenti, consulta Configuring S3 Object Lock nella Amazon S3 User Guide.

[S3.17] I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys

Categoria: Proteggi > Protezione dei dati > Crittografia dei dati archiviati

Requisiti correlati: 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 (1) NIST.800-53.r5 SC-28, (10), 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 1/3.5.1, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06, Profilo CRI v2. 2/PR. PS-01.07

Gravità: media

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-default-encryption-kms

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un bucket Amazon S3 per uso generico è crittografato con un AWS KMS key (SSE-KMS o). DSSE-KMS Il controllo fallisce se il bucket è crittografato con la crittografia predefinita (). SSE-S3

Server-side la crittografia (SSE) è la crittografia dei dati a destinazione da parte dell'applicazione o del servizio che li riceve. Se non diversamente specificato, i bucket S3 utilizzano le chiavi gestite di Amazon S3 SSE-S3 () per impostazione predefinita per la crittografia lato server. Tuttavia, per un maggiore controllo, puoi scegliere di configurare i bucket per utilizzare invece la crittografia lato server con (o). AWS KMS keys SSE-KMS DSSE-KMS Amazon S3 crittografa i tuoi dati a livello di oggetto mentre li scrive su dischi nei data AWS center e li decrittografa per te quando ti accedi.

Correzione

Per crittografare un bucket S3 utilizzando SSE-KMS, consulta Specificing server-side encryption with () AWS KMS nella Amazon S3 User SSE-KMS Guide. Per crittografare un bucket S3 utilizzando DSSE-KMS, consulta Specificare la crittografia lato server a doppio livello con () AWS KMS keys nella DSSE-KMS Amazon S3 User Guide.

[S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate

Requisiti correlati: 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, Profilo CRI v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-04.01, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01

Categoria: Protezione > Gestione sicura degli accessi > Risorsa non accessibile al pubblico

Severità: critica

Tipo di risorsa: `AWS::S3::AccessPoint`

Regola AWS Config : s3-access-point-public-access-blocks

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un punto di accesso Amazon S3 ha abilitato le impostazioni di blocco dell'accesso pubblico. Il controllo fallisce se le impostazioni di blocco dell'accesso pubblico non sono abilitate per il punto di accesso.

La funzionalità Amazon S3 Block Public Access ti aiuta a gestire l'accesso alle tue risorse S3 a tre livelli: account, bucket e access point. Le impostazioni a ciascun livello possono essere configurate in modo indipendente, consentendoti di avere diversi livelli di restrizioni di accesso pubblico ai tuoi dati. Le impostazioni del punto di accesso non possono sovrascrivere individualmente le impostazioni più restrittive ai livelli superiori (livello di account o bucket assegnato al punto di accesso). Al contrario, le impostazioni a livello del punto di accesso sono additive, il che significa che completano e funzionano insieme alle impostazioni degli altri livelli. A meno che tu non voglia che un punto di accesso S3 sia accessibile al pubblico, devi abilitare le impostazioni di blocco dell'accesso pubblico.

Correzione

Amazon S3 attualmente non supporta la modifica delle impostazioni di blocco dell'accesso pubblico di un punto di accesso dopo la creazione del punto di accesso. Tutte le impostazioni di blocco dell'accesso pubblico sono abilitate per impostazione predefinita quando crei un nuovo punto di accesso. È consigliabile lasciare tutte le impostazioni abilitate, a meno che tu non debba necessariamente disabilitarne una specifica. Per ulteriori informazioni, consulta la sezione Gestione dell'accesso pubblico agli access point nella Guida per l'utente di Amazon Simple Storage Service.

[S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/2.1.2, benchmark AWS CIS Foundations v3.0. 0/2.1.2, benchmark AWS CIS Foundations v1.4. 0/2.1.3, NIST.800-53.r5 CA-9 (1), (2) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), (2) NIST.800-53.r5 CM-3, Profilo NIST.800-53.r5 SC-5 CRI v2. 2/PR. AA-03.01, Profilo CRI v2. 2/PR. AA-05.02, Profilo CRI v2. 2/PR. DS-01.01

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: bassa

Tipo di risorsa: `AWS::S3::Bucket`

Regola AWS Config : s3-bucket-mfa-delete-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'eliminazione dell'autenticazione a più fattori (MFA) è abilitata per un bucket Amazon S3 generico. Il controllo fallisce se l'eliminazione MFA non è abilitata per il bucket. Il controllo non produce risultati per i bucket con una configurazione del ciclo di vita.

Se abiliti il controllo delle versioni per un bucket S3 generico, puoi facoltativamente aggiungere un altro livello di sicurezza configurando l'eliminazione MFA per il bucket. In tal caso, il proprietario del bucket deve includere due forme di autenticazione in ogni richiesta per eliminare una versione di un oggetto nel bucket o modificare lo stato di controllo delle versioni del bucket. L'eliminazione MFA fornisce una maggiore sicurezza se, ad esempio, le credenziali di sicurezza del proprietario del bucket sono compromesse. L'eliminazione MFA può anche aiutare a prevenire le eliminazioni accidentali dei bucket richiedendo all'utente che avvia l'azione di eliminazione di dimostrare il possesso fisico di un dispositivo MFA con un codice MFA, che aggiunge un ulteriore livello di attrito e sicurezza all'azione di eliminazione.

> **Note**
>
> Questo controllo produce un `PASSED` risultato solo se l'eliminazione MFA è abilitata per il bucket generico S3. Per abilitare l'eliminazione MFA per un bucket, è necessario abilitare anche il controllo delle versioni per il bucket. Il controllo delle versioni del bucket è un metodo per archiviare più varianti di un oggetto S3 nello stesso bucket. Inoltre, solo il proprietario del bucket che ha effettuato l'accesso come utente root può abilitare l'eliminazione MFA ed eseguire azioni di eliminazione sul bucket. Non è possibile utilizzare MFA delete con un bucket con una configurazione del ciclo di vita.

Correzione

Per informazioni sull'abilitazione del controllo delle versioni e sulla configurazione dell'eliminazione MFA per un bucket S3, consulta Configuring MFA delete nella Amazon Simple Storage Service User Guide.

[S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/3.8, benchmark AWS CIS Foundations v3.0. 0/3.8, PCI DSS versione 4.0. 1/10.2.1, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/PR. PS-04.02

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS:::Account`

Regola AWS Config : cloudtrail-all-write-s3-data-event-check

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un utente Account AWS dispone di almeno un percorso AWS CloudTrail multiregionale che registra tutti gli eventi di scrittura dei dati per i bucket Amazon S3. Il controllo fallisce se l'account non dispone di un percorso multiregionale che registra gli eventi di scrittura dei dati per i bucket S3.

Le operazioni a livello di oggetto S3, ad esempio, e, sono chiamate eventi relativi ai `GetObject` dati`DeleteObject`. `PutObject` Per impostazione predefinita, CloudTrail non registra gli eventi relativi ai dati, ma puoi configurare percorsi per registrare gli eventi relativi ai dati per i bucket S3. Quando abiliti la registrazione a livello di oggetto per gli eventi di scrittura dei dati, puoi registrare l'accesso a ogni singolo oggetto (file) all'interno di un bucket S3. L'abilitazione della registrazione a livello di oggetto può aiutarti a soddisfare i requisiti di conformità dei dati, eseguire analisi di sicurezza complete, monitorare modelli specifici di comportamento degli utenti e intervenire sull'attività delle API a livello di oggetto all'interno dei tuoi bucket S3 utilizzando Amazon Events. Account AWS CloudWatch Questo controllo produce un `PASSED` risultato se configuri un percorso multiregionale che registra eventi di sola scrittura o tutti i tipi di dati per tutti i bucket S3.

Correzione

Per abilitare la registrazione a livello di oggetto per i bucket S3, consulta Enabling CloudTrail event logging for S3 bucket and objects nella Amazon Simple Storage Service User Guide.

[S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto

Requisiti correlati: CIS AWS Foundations Benchmark v5.0. 0/3.9, benchmark AWS CIS Foundations v3.0. 0/3.9, PCI DSS versione 4.0. 1/10.2.1, Profilo CRI v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. AE-07.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. AN-07.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS:::Account`

Regola AWS Config : cloudtrail-all-read-s3-data-event-check

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un utente Account AWS dispone di almeno un percorso AWS CloudTrail multiregionale che registra tutti gli eventi di lettura dei dati per i bucket Amazon S3. Il controllo fallisce se l'account non dispone di un percorso multiregionale che registra gli eventi dei dati di lettura per i bucket S3.

Le operazioni a livello di oggetto S3, ad esempio, e, sono chiamate eventi relativi ai `GetObject` dati`DeleteObject`. `PutObject` Per impostazione predefinita, CloudTrail non registra gli eventi relativi ai dati, ma puoi configurare percorsi per registrare gli eventi relativi ai dati per i bucket S3. Quando abiliti la registrazione a livello di oggetto per gli eventi di lettura dei dati, puoi registrare l'accesso a ogni singolo oggetto (file) all'interno di un bucket S3. L'abilitazione della registrazione a livello di oggetto può aiutarti a soddisfare i requisiti di conformità dei dati, eseguire analisi di sicurezza complete, monitorare modelli specifici di comportamento degli utenti e intervenire sull'attività delle API a livello di oggetto all'interno dei tuoi bucket S3 utilizzando Amazon Events. Account AWS CloudWatch Questo controllo produce `PASSED` risultati se configuri un percorso multiregionale che registra eventi di sola lettura o tutti i tipi di eventi relativi ai dati per tutti i bucket S3.

Correzione

Per abilitare la registrazione a livello di oggetto per i bucket S3, consulta Enabling CloudTrail event logging for S3 bucket and objects nella Amazon Simple Storage Service User Guide.

[S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate

Requisiti correlati: PCI DSS v4.0. 1/14.4.4, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. IR-01.01

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::S3::MultiRegionAccessPoint`

AWS Config regola: `s3-mrap-public-access-blocked` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un punto di Multi-Region accesso Amazon S3 ha abilitato le impostazioni di blocco dell'accesso pubblico. Il controllo fallisce quando nell' Multi-Region Access Point non sono abilitate le impostazioni di blocco dell'accesso pubblico.

Le risorse accessibili al pubblico possono comportare accessi non autorizzati, violazioni dei dati o sfruttamento di vulnerabilità. Limitare l'accesso tramite misure di autenticazione e autorizzazione aiuta a salvaguardare le informazioni sensibili e a mantenere l'integrità delle risorse.

Correzione

Per impostazione predefinita, tutte le impostazioni Block Public Access sono abilitate per un punto di accesso S3 Multi-Region . Per ulteriori informazioni, consulta Bloccare l'accesso pubblico con punti di accesso Amazon S3 nella Multi-Region Guida per l'utente di Amazon Simple Storage Service. Non puoi modificare le impostazioni di Block Public Access per un Multi-Region Access Point dopo che è stato creato.

[S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita

Categoria: Proteggi > Protezione dei dati

Gravità: bassa

Tipo di risorsa: `AWS::S3Express::DirectoryBucket`

Regola AWS Config : s3express-dir-bucket-lifecycle-rules-check

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`targetExpirationDays`	Il numero di giorni, dopo la creazione dell'oggetto, in cui gli oggetti devono scadere.	Numero intero	Da 1 a 2147483647	Nessun valore predefinito

Questo controllo verifica se le regole del ciclo di vita sono configurate per un bucket di directory S3. Il controllo fallisce se le regole del ciclo di vita non sono configurate per il bucket di directory o se una regola del ciclo di vita per il bucket specifica impostazioni di scadenza che non corrispondono al valore del parametro specificato facoltativamente.

In Amazon S3, una configurazione del ciclo di vita è un insieme di regole che definiscono le azioni che Amazon S3 deve applicare a un gruppo di oggetti in un bucket. Per un bucket di directory S3, puoi creare una regola del ciclo di vita che specifica quando gli oggetti scadono in base all'età (in giorni). Puoi anche creare una regola del ciclo di vita che elimini i caricamenti multiparte incompleti. A differenza di altri tipi di bucket S3, come i bucket generici, i bucket di directory non supportano altri tipi di azioni per le regole del ciclo di vita, come la transizione di oggetti tra classi di storage.

Correzione

Per definire una configurazione del ciclo di vita per un bucket di directory S3, crea una regola del ciclo di vita per il bucket. Per ulteriori informazioni, consulta Creazione e gestione di una configurazione del ciclo di vita per il tuo bucket di directory nella Guida per l'utente di Amazon Simple Storage Service.

Controlli CSPM di Security Hub per l'IA SageMaker

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse di Amazon SageMaker AI. I controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet

Requisiti correlati: 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. 1/1.2.1, PCI DSS versione 3.2. 1/1.3.1, PCI DSS versione 3.2. 1/1.3.2, PCI DSS versione 3.2. 1/1.3.4, PCI DSS versione 3.2. 1/1.3.6, PCI DSS versione 4.0. 1/1.4.4, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.01

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: `AWS::SageMaker::NotebookInstance`

Regola AWS Config : sagemaker-notebook-no-direct-internet-access

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se l'accesso diretto a Internet è disabilitato per un'istanza di notebook SageMaker AI. Il controllo fallisce se il `DirectInternetAccess` campo è abilitato per l'istanza del notebook.

Se configuri la tua istanza SageMaker AI senza un VPC, per impostazione predefinita è abilitato l'accesso diretto a Internet sull'istanza. È necessario configurare l'istanza con un VPC e modificare l'impostazione predefinita su Disabilita: accedi a Internet tramite un VPC. Per addestrare o ospitare modelli da un notebook, è necessario l'accesso a Internet. Per abilitare l'accesso a Internet, il VPC deve disporre di un endpoint di interfaccia (AWS PrivateLink) o di un gateway NAT e di un gruppo di sicurezza che consenta le connessioni in uscita. Per ulteriori informazioni su come connettere un'istanza di notebook alle risorse in un VPC, consulta Connettere un'istanza di notebook alle risorse in un VPC nella Amazon SageMaker AI Developer Guide. Dovresti inoltre assicurarti che l'accesso alla tua configurazione SageMaker AI sia limitato ai soli utenti autorizzati. Limita le autorizzazioni IAM che consentono agli utenti di modificare le impostazioni e le risorse SageMaker AI.

Correzione

Non è possibile modificare l'impostazione di accesso a Internet dopo aver creato un'istanza di notebook. Puoi invece interrompere, eliminare e ricreare l'istanza con accesso a Internet bloccato. Per eliminare un'istanza di notebook che consente l'accesso diretto a Internet, consulta Use notebook instances to build models: Clean up nella Amazon SageMaker AI Developer Guide. Per ricreare un'istanza di notebook che nega l'accesso a Internet, consulta Creare un'istanza notebook. Per Rete, accesso diretto a Internet, scegli Disabilita: accedi a Internet tramite un VPC.

[SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato

Requisiti correlati: 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), (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 Profile v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Gravità: alta

Tipo di risorsa: `AWS::SageMaker::NotebookInstance`

Regola AWS Config : sagemaker-notebook-instance-inside-vpc

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istanza di notebook Amazon SageMaker AI viene avviata all'interno di un cloud privato virtuale (VPC) personalizzato. Questo controllo fallisce se un'istanza di notebook SageMaker AI non viene avviata all'interno di un VPC personalizzato o se viene avviata nel servizio SageMaker AI VPC.

Le sottoreti sono un intervallo di indirizzi IP all'interno di un VPC. Ti consigliamo di mantenere le tue risorse all'interno di un VPC personalizzato quando possibile per garantire una protezione di rete sicura della tua infrastruttura. Un Amazon VPC è una rete virtuale dedicata al tuo. Account AWS Con Amazon VPC, puoi controllare l'accesso alla rete e la connettività Internet delle tue istanze di SageMaker AI Studio e notebook.

Correzione

Non è possibile modificare l'impostazione del VPC dopo aver creato un'istanza del notebook. Puoi invece interrompere, eliminare e ricreare l'istanza. Per istruzioni, consulta Usare le istanze di notebook per creare modelli: pulisci nella Amazon SageMaker AI Developer Guide.

[SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook

Requisiti correlati: 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, Profilo CRI v2. 2/PR. AA-05.02

Categoria: Protezione > Gestione sicura degli accessi > Restrizioni all'accesso degli utenti root

Gravità: alta

Tipo di risorsa: `AWS::SageMaker::NotebookInstance`

Regola AWS Config : sagemaker-notebook-instance-root-access-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'accesso root è attivato per un'istanza di notebook Amazon SageMaker AI. Il controllo fallisce se l'accesso root è attivato per un'istanza di notebook SageMaker AI.

In conformità al principio del privilegio minimo, è consigliabile limitare l'accesso root alle risorse dell'istanza per evitare involontariamente il sovraassegnamento delle autorizzazioni.

Correzione

Per limitare l'accesso root alle istanze di notebook SageMaker AI, consulta Controllare l'accesso root a un'istanza di notebook SageMaker AI nella Amazon SageMaker AI Developer Guide.

[SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1

Requisiti correlati: 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, Profilo CRI v2. 2/PR. IR-04.02

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::SageMaker::EndpointConfig`

Regola AWS Config : sagemaker-endpoint-config-prod-instance-count

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se le varianti di produzione di un endpoint Amazon SageMaker AI hanno un numero iniziale di istanze superiore a 1. Il controllo fallisce se le varianti di produzione dell'endpoint hanno solo 1 istanza iniziale.

Le varianti di produzione eseguite con un numero di istanze superiore a 1 consentono la ridondanza delle istanze Multi-AZ gestita dall'IA. SageMaker L'implementazione di risorse su più zone di disponibilità è una AWS best practice per fornire un'elevata disponibilità all'interno dell'architettura. L'elevata disponibilità consente di riprendersi dagli incidenti di sicurezza.

> **Note**
>
> Questo controllo si applica solo alla configurazione degli endpoint basata sull'istanza.

Correzione

Per ulteriori informazioni sui parametri di configurazione degli endpoint, consulta Create an endpoint configuration nella Amazon SageMaker AI Developer Guide.

[SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato

Requisiti correlati: CRI Profile v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: media

Tipo di risorsa: `AWS::SageMaker::Model`

Regola AWS Config : sagemaker-model-isolation-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un modello ospitato da Amazon SageMaker AI ha l'isolamento di rete abilitato. Il controllo fallisce se il `EnableNetworkIsolation` parametro per il modello ospitato è impostato su`False`.

SageMaker La formazione sull'intelligenza artificiale e i contenitori di inferenza distribuiti sono abilitati a Internet per impostazione predefinita. Se non vuoi che l' SageMaker intelligenza artificiale fornisca l'accesso alla rete esterna ai tuoi contenitori di formazione o inferenza, puoi abilitare l'isolamento della rete. Se abiliti l'isolamento della rete, non è possibile effettuare chiamate di rete in entrata o in uscita da o verso il contenitore del modello, incluse le chiamate da o verso altri. Servizi AWS Inoltre, non vengono rese disponibili AWS credenziali per l'ambiente di runtime del contenitore. L'abilitazione dell'isolamento della rete aiuta a prevenire l'accesso involontario alle risorse di SageMaker intelligenza artificiale da Internet.

> **Note**
>
> Il 13 agosto 2025, Security Hub CSPM ha cambiato il titolo e la descrizione di questo controllo. Il nuovo titolo e la nuova descrizione riflettono in modo più accurato che il controllo verifica l'impostazione del `EnableNetworkIsolation` parametro dei modelli ospitati da

Amazon SageMaker AI. In precedenza, il titolo di questo controllo era: SageMaker models should block inbound traffic.

Correzione

Per ulteriori informazioni sull'isolamento della rete per i modelli di SageMaker intelligenza artificiale, consulta Esegui contenitori di formazione e inferenza in modalità senza Internet nella Amazon SageMaker AI Developer Guide. Quando crei un modello, puoi abilitare l'isolamento della rete impostando il valore del parametro su. `EnableNetworkIsolation` `True`

[SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::SageMaker::AppImageConfig`

Regola AWS Config : sagemaker-app-image-config-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se la configurazione dell'immagine di un'app Amazon SageMaker AI (`AppImageConfig`) ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo

fallisce se la configurazione dell'immagine dell'app non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la configurazione dell'immagine dell'app non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per aggiungere tag a una configurazione dell'immagine di un'app Amazon SageMaker AI (`AppImageConfig`), puoi utilizzare il AddTagsfunzionamento dell'API SageMaker AI o, se utilizzi il AWS CLI, eseguire il comando add-tags.

[SageMaker.7] SageMaker le immagini devono essere taggate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::SageMaker::Image`

Regola AWS Config : sagemaker-image-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un'immagine Amazon SageMaker AI ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo fallisce se l'immagine non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'immagine non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per aggiungere tag a un'immagine Amazon SageMaker AI, puoi utilizzare il AddTagsfunzionamento dell'API SageMaker AI o, se utilizzi il AWS CLI, eseguire il comando add-tags.

[SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate

Requisiti correlati: CRI Profile v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-02.02

Categoria: Rileva > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: `AWS::SageMaker::NotebookInstance`

Regola AWS Config : sagemaker-notebook-instance-platform-version

Tipo di pianificazione: periodica

Parametri:

- `supportedPlatformIdentifierVersions`: `notebook-al2023-v1` (non personalizzabile)

Questo controllo verifica se un'istanza di notebook Amazon SageMaker AI è configurata per l'esecuzione su una piattaforma supportata, in base all'identificatore della piattaforma specificato per l'istanza del notebook. Il controllo fallisce se l'istanza del notebook è configurata per l'esecuzione su una piattaforma che non è più supportata.

Se la piattaforma per un'istanza di notebook Amazon SageMaker AI non è più supportata, potrebbe non ricevere patch di sicurezza, correzioni di bug o altri tipi di aggiornamenti. Le istanze notebook potrebbero continuare a funzionare, ma non riceveranno aggiornamenti di sicurezza SageMaker AI o correzioni di bug critici. Ti assumi i rischi associati all'utilizzo di una piattaforma non supportata. Per ulteriori informazioni, consulta il JupyterLabcontrollo delle versioni nella Amazon SageMaker AI Developer Guide.

Correzione

Per informazioni sulle piattaforme attualmente supportate da Amazon SageMaker AI e su come migrare verso di esse, consulta le istanze di notebook Amazon Linux 2 nella Amazon SageMaker AI Developer Guide.

[SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container

Categoria: Proteggi > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::SageMaker::DataQualityJobDefinition`

Regola AWS Config : sagemaker-data-quality-job-encrypt-in-transit

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una definizione di processo di qualità dei dati di Amazon SageMaker AI ha la crittografia abilitata per il traffico tra container. Il controllo fallisce se la definizione di un processo che monitora la qualità e la deriva dei dati non ha la crittografia abilitata per il traffico tra container.

L'abilitazione della crittografia del traffico tra container protegge i dati ML sensibili durante l'elaborazione distribuita per l'analisi della qualità dei dati.

Correzione

Per ulteriori informazioni sulla crittografia del traffico tra container per Amazon SageMaker AI, consulta Protect Communications Between ML Compute Instances in a Distributed Training Job nella Amazon SageMaker AI Developer Guide. Quando crei una definizione di processo per la qualità dei dati, puoi abilitare la crittografia del traffico tra container impostando il valore del parametro su. `EnableInterContainerTrafficEncryption` `True`

[SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::SageMaker::ModelExplainabilityJobDefinition`

Regola AWS Config : sagemaker-model-explainability-job-encrypt-in-transit

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una definizione di processo di spiegabilità SageMaker del modello Amazon ha abilitata la crittografia del traffico tra container. Il controllo fallisce se la definizione del processo di spiegabilità del modello non ha abilitato la crittografia del traffico tra container.

L'attivazione della crittografia del traffico tra container protegge i dati ML sensibili come i dati del modello, i set di dati di addestramento, i risultati di elaborazione intermedi, i parametri e i pesi dei modelli durante l'elaborazione distribuita per l'analisi della spiegabilità.

Correzione

Per quanto riguarda la definizione di un lavoro di spiegabilità SageMaker del modello esistente, la crittografia del traffico tra container non può essere aggiornata. Per creare una nuova definizione di processo di spiegabilità del SageMaker modello con la crittografia del traffico tra container abilitata, utilizza l'API o la CLI o e imposta su. CloudFormation`EnableInterContainerTrafficEncryption``True`

[SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: `AWS::SageMaker::DataQualityJobDefinition`

Regola AWS Config : sagemaker-data-quality-job-isolation

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una definizione di processo di monitoraggio della qualità dei dati di Amazon SageMaker AI ha l'isolamento della rete abilitato. Il controllo fallisce se l'isolamento della rete è disabilitato nella definizione di un processo che monitora la qualità e la deriva dei dati.

L'isolamento della rete riduce la superficie di attacco e impedisce l'accesso esterno, proteggendo in tal modo da accessi esterni non autorizzati, esposizione accidentale dei dati e potenziale esfiltrazione dei dati.

Correzione

Per ulteriori informazioni sull'isolamento della rete per l' SageMaker intelligenza artificiale, consulta Esegui contenitori di formazione e inferenza in modalità senza Internet nella Amazon SageMaker AI Developer Guide. Quando crei una definizione di processo per la qualità dei dati, puoi abilitare l'isolamento della rete impostando il valore del parametro su. `EnableNetworkIsolation` `True`

[SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato

Categoria: Protezione > Configurazione sicura della rete > Configurazione della politica delle risorse

Gravità: media

Tipo di risorsa: `AWS::SageMaker::ModelBiasJobDefinition`

Regola AWS Config : sagemaker-model-bias-job-isolation

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una definizione di job di polarizzazione SageMaker del modello ha l'isolamento della rete abilitato. Il controllo fallisce se nella definizione del processo di polarizzazione del modello non è abilitato l'isolamento della rete.

L'isolamento della rete impedisce ai job di SageMaker model bias di comunicare con risorse esterne su Internet. Abilitando l'isolamento della rete, vi assicurate che i container del job non possano effettuare connessioni in uscita, riducendo la superficie di attacco e proteggendo i dati sensibili dall'esfiltrazione. Ciò è particolarmente importante per i lavori che trattano dati regolamentati o sensibili.

Correzione

Per abilitare l'isolamento della rete, è necessario creare una nuova definizione di job di polarizzazione del modello con il `EnableNetworkIsolation` parametro impostato `True` su. L'isolamento della rete non può essere modificato dopo la creazione della definizione del processo. Per creare una nuova definizione di job basato su modelli, consulta CreateModelBiasJobDefinitionla Amazon SageMaker AI Developer Guide.

[SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata

Categoria: Proteggi > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::SageMaker::ModelQualityJobDefinition`

Regola AWS Config : ssagemaker-model-quality-job-encrypt-in-transit

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le definizioni dei processi di qualità dei SageMaker modelli Amazon hanno la crittografia in transito abilitata per il traffico tra container. Il controllo fallisce se una definizione di processo di qualità del modello non ha abilitato la crittografia del traffico tra container.

Inter-container la crittografia del traffico protegge i dati trasmessi tra i contenitori durante i lavori di monitoraggio della qualità dei modelli distribuiti. Per impostazione predefinita, il traffico tra container non è crittografato. L'attivazione della crittografia aiuta a mantenere la riservatezza dei dati durante l'elaborazione e supporta la conformità ai requisiti normativi per la protezione dei dati in transito.

Correzione

Per abilitare la crittografia del traffico tra container per la definizione del processo di qualità SageMaker del modello Amazon, devi ricreare la definizione del processo con la configurazione di crittografia in transito appropriata. Per creare una definizione di lavoro di qualità del modello, CreateModelQualityJobDefinitionconsulta la Amazon SageMaker AI Developer Guide.

[SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: `AWS::SageMaker::MonitoringSchedule`

Regola AWS Config : sagemaker-monitoring-schedule-isolation

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se nei piani di SageMaker monitoraggio di Amazon è abilitato l'isolamento della rete. Il controllo fallisce se una pianificazione di monitoraggio è EnableNetworkIsolation impostata su false o non è configurata

L'isolamento della rete impedisce ai job di monitoraggio di effettuare chiamate di rete in uscita, riducendo la superficie di attacco eliminando l'accesso a Internet dai container.

Correzione

Per informazioni sulla configurazione dell'isolamento della rete nel NetworkConfig parametro durante la creazione o l'aggiornamento di una pianificazione di monitoraggio, consulta CreateMonitoringScheduleo UpdateMonitoringScheduleconsulta la Amazon SageMaker AI Developer Guide.

[SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::SageMaker::ModelBiasJobDefinition`

Regola AWS Config : sagemaker-model-bias-job-encrypt-in-transit

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se nelle definizioni dei job di Amazon SageMaker model bias è abilitata la crittografia del traffico tra container quando si utilizzano più istanze di calcolo. Il controllo ha esito negativo se `EnableInterContainerTrafficEncryption` è impostato su false o non è configurato per le definizioni dei processi con un numero di istanze pari o superiore a 2.

Inter-container la crittografia del traffico protegge i dati trasmessi tra le istanze di calcolo durante i processi di monitoraggio della distorsione del modello distribuito. La crittografia impedisce l'accesso

non autorizzato alle informazioni relative al modello, ad esempio i pesi, che vengono trasmessi tra le istanze.

Correzione

Per abilitare la crittografia del traffico tra container per le definizioni dei processi di distorsione dei SageMaker modelli, imposta il `EnableInterContainerTrafficEncryption` parametro su `True` quando la definizione del processo utilizza più istanze di calcolo. Per informazioni sulla protezione delle comunicazioni tra istanze di calcolo ML, consulta Protect Communications Between ML Compute Instances in a Distributed Training Job nella Amazon SageMaker AI Developer Guide.

[SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Gravità: media

Tipo di risorsa: `AWS::SageMaker::Model`

Regola AWS Config : sagemaker-model-private-registry-required

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un modello Amazon SageMaker AI estrae l'immagine del contenitore da un registro privato in un VPC per il contenitore principale. Il controllo fallisce se l'immagine non è configurata o la modalità di accesso al repository è attiva. `Platform`

L'utilizzo di un registro Docker privato in un VPC SageMaker per container modello garantisce che le immagini dei container vengano estratte da fonti affidabili e controllate all'interno del VPC. Inoltre, garantisce l'accesso alle immagini dei container tramite endpoint VPC, senza attraversare la rete Internet pubblica.

Correzione

Per configurare registri docker privati per contenitori di inferenza SageMaker AI in tempo reale, consulta Use a Private Docker Registry for Inference Real-Time Containers nella Amazon AI Developer Guide. SageMaker

[SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::SageMaker::FeatureGroup`

Regola AWS Config : sagemaker-featuregroup-encryption-at-rest

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un negozio SageMaker offline Amazon per un gruppo di funzionalità è crittografato a riposo con una AWS KMS chiave. Il controllo fallisce se lo storage S3 dello store offline per un gruppo di funzionalità non è crittografato con una chiave KMS.

L'utilizzo della crittografia gestita dal cliente AWS KMS keys negli altri negozi offline del gruppo di SageMaker funzionalità offre una maggiore sicurezza. Customer-managed Le chiavi KMS offrono il pieno controllo sul ciclo di vita delle chiavi di crittografia e sulle politiche chiave. Inoltre, tutto l'utilizzo delle chiavi di crittografia può essere registrato e monitorato per verificarne la verificabilità. AWS CloudTrail

Correzione

Per informazioni sull'attivazione della crittografia a riposo per i negozi offline del SageMaker Feature Store utilizzando chiavi AWS KMS gestite dal cliente, consulta Sicurezza e controllo degli accessi nella Amazon SageMaker AI Developer Guide.

[SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys

Requisiti correlati: 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)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: `AWS::SageMaker::FeatureGroup`

Regola AWS Config : sagemaker-featuregroup-online-store-encryption

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un negozio SageMaker online Amazon per un gruppo di funzionalità con archiviazione standard è crittografato a riposo con una AWS KMS chiave. Il controllo fallisce se la crittografia con chiave KMS non è configurata per il negozio online.

L'utilizzo della crittografia gestita dal cliente AWS KMS keys negli altri negozi online del gruppo di SageMaker funzionalità offre una maggiore sicurezza. Customer-managed Le chiavi KMS offrono il pieno controllo sul ciclo di vita delle chiavi di crittografia e sulle politiche chiave. Inoltre, tutto l'utilizzo delle chiavi di crittografia può essere registrato e monitorato per verificarne la verificabilità. AWS CloudTrail

Correzione

Per informazioni sull'attivazione della crittografia a riposo per i negozi online SageMaker Feature Store utilizzando chiavi AWS KMS gestite dal cliente, consulta Sicurezza e controllo degli accessi nella Amazon SageMaker AI Developer Guide.

[SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Gravità: media

Tipo di risorsa: `AWS::SageMaker::Model`

Regola AWS Config : sagemaker-model-multicontainer-private-registry

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i modelli Amazon SageMaker AI con pipeline di inferenza multi-contenitore estraggono le immagini dei container da un registro Docker privato in un VPC. Il controllo

fallisce se una definizione di contenitore non ha una configurazione di immagine o se la modalità di accesso al repository è impostata sulla piattaforma.

L'utilizzo di un registro Docker privato in una pipeline di inferenza multi-contenitore VPC SageMaker for AI garantisce che le immagini dei container vengano estratte da fonti affidabili e controllate all'interno del VPC. Ciò garantisce l'accesso alle immagini dei container tramite endpoint VPC, senza attraversare la rete Internet pubblica, riducendo il rischio di attacchi alla catena di approvvigionamento o manomissioni delle immagini.

Correzione

Per configurare registri docker privati per contenitori di inferenza SageMaker AI in tempo reale, consulta Use a Private Docker Registry for Inference Real-Time Containers nella Amazon AI Developer Guide. SageMaker

[SageMaker.20] le definizioni dei lavori di spiegabilità dei SageMaker modelli dovrebbero avere l'isolamento della rete abilitato

Categoria: Protezione > Configurazione sicura della rete > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::SageMaker::ModelExplainabilityJobDefinition`

Regola AWS Config : sagemaker-model-explainability-job-network-isolation

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una definizione di processo di spiegabilità di un modello di SageMaker intelligenza artificiale ha l'isolamento della rete abilitato. Il controllo fallisce se nella definizione del processo non è abilitato l'isolamento di rete.

L'isolamento della rete impedisce ai job container di spiegabilità del modello di effettuare chiamate di rete in uscita, riducendo il rischio di esfiltrazione dei dati e fornendo una difesa approfondita per i dati sensibili del modello e della formazione.

Correzione

Per abilitare l'isolamento della rete per la definizione del processo di spiegabilità di un modello di SageMaker intelligenza artificiale, imposta su quando si crea la definizione del processo.

`NetworkConfig.EnableNetworkIsolation` `true` Per ulteriori informazioni sull'isolamento della rete per l' SageMaker intelligenza artificiale, consulta Esegui contenitori di formazione e inferenza in modalità senza Internet nella Amazon SageMaker AI Developer Guide.

[SageMaker.21] le istanze di SageMaker notebook devono essere crittografate e gestite dal cliente AWS KMS keys

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: `AWS::SageMaker::NotebookInstance`

Regola AWS Config : sagemaker-notebook-instance-storage-vol-kms-encrypted

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istanza di notebook SageMaker AI è configurata con una AWS KMS chiave per la crittografia dei volumi di archiviazione. Il controllo fallisce se una chiave KMS non è configurata per l'istanza del notebook.

La crittografia dei dati inattivi con una chiave KMS gestita dal cliente fornisce un ulteriore controllo degli accessi rispetto alla crittografia AWS gestita predefinita. SageMaker Le istanze di notebook AI archiviano i notebook degli utenti, i set di dati, gli artefatti dei modelli e i dati di elaborazione temporanea su volumi di archiviazione ML. Una chiave gestita dal cliente consente un controllo granulare delle policy chiave, la registrazione di CloudTrail verifica dell'utilizzo delle chiavi e la conformità ai framework che richiedono la crittografia controllata dal cliente.

Correzione

Per configurare una chiave KMS per un'istanza di notebook SageMaker AI, consulta Notebook instances, SageMaker AI jobs ed Endpoints nella Amazon SageMaker AI Developer Guide. Tieni presente che `KmsKeyId` può essere impostato solo al momento della creazione dell'istanza notebook. Per rimediare, crea una nuova istanza di notebook con la chiave KMS specificata ed esegui la migrazione dei dati dall'istanza esistente.

[SageMaker.22] le pianificazioni di SageMaker monitoraggio dovrebbero avere la crittografia del traffico tra container abilitata

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::SageMaker::MonitoringSchedule`

Regola AWS Config : sagemaker-monitoring-schedule-traffic-encryption

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un programma di monitoraggio di Amazon SageMaker AI ha la crittografia abilitata per il traffico tra container. Il controllo fallisce se la definizione del processo di monitoraggio non ha la crittografia abilitata per il traffico tra container.

Inter-container la crittografia del traffico garantisce che i dati trasmessi tra i contenitori durante i lavori di monitoraggio siano crittografati durante il transito. Senza questa crittografia, i dati sensibili elaborati durante il monitoraggio del modello potrebbero essere esposti ad accessi non autorizzati all'interno della rete. L'attivazione di questa impostazione aiuta a soddisfare i requisiti di conformità per la protezione dei dati in transito.

Correzione

Per un programma di monitoraggio dell' SageMaker IA esistente, la crittografia del traffico tra container non può essere aggiornata. Per creare una nuova pianificazione di monitoraggio dell' SageMaker IA con la crittografia del traffico tra container abilitata, utilizza l'API o la CLI o CloudFormation imposta su `true` in the `EnableInterContainerTrafficEncryption` of. `NetworkConfig` `MonitoringJobDefinition`

[SageMaker.23] gli esperimenti di SageMaker inferenza dovrebbero avere il volume di archiviazione delle istanze crittografato e gestito dal cliente AWS KMS keys

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: `AWS::SageMaker::InferenceExperiment`

Regola AWS Config : sagemaker-inf-experiment-instance-storage-kms-encrypted

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un esperimento di inferenza SageMaker AI è configurato con una AWS KMS chiave, ad esempio la crittografia del volume di archiviazione. Il controllo fallisce se non viene specificata una chiave KMS, ad esempio la crittografia del volume di archiviazione.

La crittografia dei volumi di archiviazione delle istanze con chiavi KMS gestite dal cliente fornisce la gestione centralizzata delle chiavi, la registrazione degli audit e il controllo della rotazione delle chiavi per gli artefatti del modello e i dati di inferenza temporanei archiviati su istanze di calcolo ML durante gli shadow test.

Correzione

Per configurare una chiave KMS per un esperimento di inferenza AI, specifica il parametro durante la chiamata SageMaker . `KmsKey` `CreateInferenceExperiment` `KmsKey`Può essere un ID chiave KMS, un ARN, un alias o un alias ARN. Il ruolo di esecuzione dell' SageMaker IA deve avere `kms:CreateGrant` l'autorizzazione sulla chiave. Per ulteriori informazioni su come specificare una AWS KMS chiave gestita dal cliente per l' SageMaker IA, consulta Notebook instances, SageMaker AI jobs ed Endpoints nella Amazon SageMaker AI Developer Guide.

[SageMaker.24] gli esperimenti di SageMaker inferenza dovrebbero avere l'archiviazione dei dati crittografata e gestita dal cliente AWS KMS keys

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: `AWS::SageMaker::InferenceExperiment`

Regola AWS Config : sagemaker-inf-experiment-data-storage-kms-encrypted

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un esperimento di inferenza SageMaker AI con acquisizione dati abilitata ha una chiave KMS configurata per crittografare i dati acquisiti a riposo. Il controllo fallisce se la configurazione di archiviazione dei dati non specifica una chiave KMS per la crittografia.

La crittografia dei dati di richiesta e risposta di inferenza acquisiti con chiavi KMS gestite dal cliente garantisce che i payload di inferenza sensibili archiviati in Amazon S3 siano protetti con funzionalità centralizzate di gestione e controllo delle chiavi.

Correzione

Per configurare una chiave KMS per l'archiviazione dei dati in un esperimento di inferenza SageMaker AI, specifica il campo all'interno della chiamata. `KmsKey` `DataStorageConfig` `CreateInferenceExperiment` `KmsKey`Crittografa i dati di richiesta di inferenza e risposta acquisiti a riposo nel bucket Amazon S3 specificato. Per ulteriori informazioni su come specificare una AWS KMS chiave gestita dal cliente per l' SageMaker IA, consulta Notebook instances, SageMaker AI jobs ed Endpoints nella Amazon SageMaker AI Developer Guide.

[SageMaker.25] le definizioni dei lavori di qualità SageMaker del modello dovrebbero avere l'isolamento della rete abilitato

Categoria: Protezione > Configurazione sicura della rete > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: `AWS::SageMaker::ModelQualityJobDefinition`

Regola AWS Config : sagemaker-model-quality-job-definition-isolation

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la definizione di un processo di qualità del modello Amazon SageMaker AI ha l'isolamento di rete abilitato. Il controllo fallisce se nella definizione del processo di qualità del modello non è abilitato l'isolamento di rete.

L'isolamento della rete riduce la superficie di attacco e impedisce l'accesso esterno, proteggendo in tal modo da accessi esterni non autorizzati, esposizione accidentale dei dati e potenziale esfiltrazione di dati.

Correzione

Quando si crea una definizione di processo di qualità del modello, è possibile abilitare l'isolamento della rete impostando il valore del parametro su. `EnableNetworkIsolation` `True` Per ulteriori informazioni sull'isolamento della rete per l' SageMaker intelligenza artificiale, consulta Esegui contenitori di formazione e inferenza in modalità senza Internet nella Amazon SageMaker AI Developer Guide.

Controlli CSPM di Security Hub per Secrets Manager

Questi AWS Security Hub CSPM controlli valutano il AWS Secrets Manager servizio e le risorse.

Questi controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[SecretsManager.1] I segreti di Secrets Manager devono avere la rotazione automatica abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/86.3, PCI DSS versione 4.0. 1/8.3.9, Profilo CRI v2. 2/PR. AA-01.01

Categoria: Protezione > Sviluppo protetto

Gravità: media

Tipo di risorsa: `AWS::SecretsManager::Secret`

Regola AWS Config : `secretsmanager-rotation-enabled-check`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`maximumAllowedRotationFrequency`	Numero massimo di giorni consentito per la frequenza di rotazione segreta	Numero intero	Da 1 a 365	Nessun valore predefinito

Questo controllo verifica se un segreto memorizzato in AWS Secrets Manager è configurato con rotazione automatica. Il controllo fallisce se il segreto non è configurato con la rotazione automatica. Se si fornisce un valore personalizzato per il `maximumAllowedRotationFrequency` parametro, il controllo passa solo se il segreto viene ruotato automaticamente all'interno della finestra temporale specificata.

Secrets Manager ti aiuta a migliorare il livello di sicurezza della tua organizzazione. I segreti includono credenziali del database, password e chiavi API di terze parti. È possibile utilizzare Secrets

Manager per archiviare i segreti centralmente, crittografarli automaticamente, controllare l'accesso ai segreti e ruotare i segreti in modo sicuro e automatico.

Secrets Manager può ruotare i segreti. È possibile utilizzare la rotazione per sostituire i segreti a lungo termine con segreti a breve termine. La rotazione dei segreti limita il tempo per cui un utente non autorizzato può utilizzare un segreto compromesso. Per questo motivo, dovresti ruotare frequentemente i tuoi segreti. Per saperne di più sulla rotazione, consulta Ruotare AWS Secrets Manager i tuoi segreti nella Guida per l'AWS Secrets Manager utente.

Correzione

Per attivare la rotazione automatica per i segreti di Secrets Manager, consulta Configurare la rotazione automatica per AWS Secrets Manager i segreti utilizzando la console nella Guida per l'AWS Secrets Manager utente. È necessario scegliere e configurare una AWS Lambda funzione per la rotazione.

[SecretsManager.2] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/86.3, PCI DSS versione 4.0. 1/8.3.9, Profilo CRI v2. 2/PR. AA-01.01

Categoria: Protezione > Sviluppo protetto

Gravità: media

Tipo di risorsa: `AWS::SecretsManager::Secret`

Regola AWS Config : `secretsmanager-scheduled-rotation-success-check`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS Secrets Manager segreto è stato ruotato correttamente in base al programma di rotazione. Il controllo fallisce se lo `RotationOccurringAsScheduled` è`false`. Il controllo valuta solo i segreti con rotazione attivata.

Secrets Manager ti aiuta a migliorare il livello di sicurezza della tua organizzazione. I segreti includono credenziali del database, password e chiavi API di terze parti. È possibile utilizzare Secrets

Manager per archiviare i segreti centralmente, crittografarli automaticamente, controllare l'accesso ai segreti e ruotare i segreti in modo sicuro e automatico.

Secrets Manager può ruotare i segreti. È possibile utilizzare la rotazione per sostituire i segreti a lungo termine con segreti a breve termine. La rotazione dei segreti limita il tempo per cui un utente non autorizzato può utilizzare un segreto compromesso. Per questo motivo, dovresti ruotare frequentemente i tuoi segreti.

Oltre a configurare i segreti in modo che ruotino automaticamente, è necessario assicurarsi che tali segreti ruotino correttamente in base alla pianificazione di rotazione.

Per ulteriori informazioni sulla rotazione, consulta Rotating your AWS Secrets Manager secret nella Guida per l'utente.AWS Secrets Manager

Correzione

Se la rotazione automatica fallisce, Secrets Manager potrebbe aver riscontrato degli errori nella configurazione. Per ruotare i segreti in Secrets Manager, si utilizza una funzione Lambda che definisce come interagire con il database o il servizio proprietario del segreto.

Per facilitare la diagnosi e la correzione degli errori comuni relativi alla rotazione dei segreti, consulta Risoluzione dei problemi relativi alla AWS Secrets Manager rotazione dei segreti nella Guida per l'AWS Secrets Manager utente.

[SecretsManager.3] Rimuovi i segreti inutilizzati di Secrets Manager

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), CRI Profile v2. 2/PR. AA-01.01, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. AA-05.03

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::SecretsManager::Secret`

Regola AWS Config : `secretsmanager-secret-unused`

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`unusedForDays`	Numero massimo di giorni in cui un segreto può rimanere inutilizzato	Numero intero	Da `1` a `365`	`90`

Questo controllo verifica se è stato effettuato l'accesso a un AWS Secrets Manager segreto entro il periodo di tempo specificato. Il controllo ha esito negativo se un segreto non viene utilizzato oltre il periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di accesso, Security Hub CSPM utilizza un valore predefinito di 90 giorni.

L'eliminazione dei segreti inutilizzati è importante tanto quanto la rotazione dei segreti. I segreti non utilizzati possono essere sfruttati in modo improprio dai precedenti utenti, che non hanno più bisogno di accedere a questi segreti. Inoltre, man mano che sempre più utenti accedono a un segreto, qualcuno potrebbe averlo gestito male e divulgato a un'entità non autorizzata, il che aumenta il rischio di abuso. L'eliminazione di segreti inutilizzati aiuta a revocare l'accesso segreto agli utenti che non ne hanno più bisogno. Inoltre aiuta a ridurre i costi di utilizzo di Secrets Manager. Pertanto, è essenziale eliminare regolarmente i segreti non utilizzati.

Correzione

Per eliminare i segreti inattivi di Secrets Manager, consulta Eliminare un AWS Secrets Manager segreto nella Guida per l'AWS Secrets Manager utente.

[SecretsManager.4] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/86.3, PCI DSS versione 4.0. 1/8.3.9, Profilo CRI v2. 2/PR. AA-01.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::SecretsManager::Secret`

Regola AWS Config : `secretsmanager-secret-periodic-rotation`

Tipo di pianificazione: periodica

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`maxDaysSinceRotation`	Numero massimo di giorni in cui un segreto può rimanere invariato	Numero intero	Da `1` a `180`	`90`

Questo controllo verifica se un AWS Secrets Manager segreto viene ruotato almeno una volta nell'intervallo di tempo specificato. Il controllo fallisce se un segreto non viene ruotato almeno così frequentemente. A meno che non si fornisca un valore di parametro personalizzato per il periodo di rotazione, Security Hub CSPM utilizza un valore predefinito di 90 giorni.

La rotazione dei segreti può aiutarti a ridurre il rischio di un uso non autorizzato dei tuoi segreti nel tuo. Account AWS Gli esempi includono credenziali di database, password, chiavi API di terze parti e persino testo arbitrario. Se non modifichi i tuoi segreti per un lungo periodo di tempo, è più probabile che i segreti vengano compromessi.

Man mano che sempre più utenti accedono a un segreto, è più probabile che qualcuno lo abbia gestito male e lo abbia divulgato a un'entità non autorizzata. I segreti possono essere fatti trapelare attraverso i log e i dati della cache. Possono essere condivisi per scopi di debug e non modificati o revocati una volta completato il debug. Per tutti questi motivi, i segreti dovrebbero essere ruotati frequentemente.

È possibile configurare la rotazione automatica dei segreti in. AWS Secrets Manager Con la rotazione automatica, è possibile sostituire i segreti a lungo termine con segreti a breve termine, riducendo notevolmente il rischio di compromissione. Ti consigliamo di configurare la rotazione automatica per i tuoi segreti di Secrets Manager. Per ulteriori informazioni, consulta Rotazione dei segreti AWS Secrets Manager nella Guida per l'utente di AWS Secrets Manager .

Correzione

Per attivare la rotazione automatica per i segreti di Secrets Manager, consulta Configurare la rotazione automatica per AWS Secrets Manager i segreti utilizzando la console nella Guida per

l'AWS Secrets Manager utente. È necessario scegliere e configurare una AWS Lambda funzione per la rotazione.

[SecretsManager.5] I segreti di Secrets Manager devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::SecretsManager::Secret`

AWS Config regola: `tagged-secretsmanager-secret` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un AWS Secrets Manager segreto contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il segreto non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il segreto non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un segreto di Secrets Manager, consulta Tag AWS Secrets Manager secrets nella Guida AWS Secrets Manager per l'utente.

Controlli CSPM Security Hub per AWS Service Catalog

Questo AWS Security Hub CSPM controllo valuta il AWS Service Catalog servizio e le risorse. Il controllo potrebbe non essere disponibile in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione

Requisiti correlati: 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, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: `AWS::ServiceCatalog::Portfolio`

Regola AWS Config : service-catalog-shared-within-organization

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se AWS Service Catalog condivide i portafogli all'interno di un'organizzazione quando l'integrazione con AWS Organizations è abilitata. Il controllo fallisce se i portafogli non sono condivisi all'interno di un'organizzazione.

La condivisione del portafoglio solo all'interno di Organizations aiuta a garantire che un portafoglio non venga condiviso con persone errate Account AWS. Per condividere un portafoglio Service Catalog con un account in un'organizzazione, Security Hub CSPM consiglia di utilizzare `ORGANIZATION_MEMBER_ACCOUNT` invece di. `ACCOUNT` Ciò semplifica l'amministrazione regolando l'accesso concesso all'account in tutta l'organizzazione. Se hai l'esigenza aziendale di condividere i portafogli Service Catalog con un account esterno, puoi eliminare automaticamente i risultati da questo controllo o disabilitarlo.

Correzione

Per abilitare la condivisione del portafoglio con AWS Organizations, consulta Condivisione con AWS Organizations nella Guida per l'AWS Service Catalog amministratore.

Controlli CSPM del Security Hub per Amazon SES

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon Simple Email Service (Amazon SES).

Questi controlli potrebbero non essere disponibili tuttiRegioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[SES.1] Gli elenchi di contatti SES devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::SES::ContactList`

AWS Configregola: `tagged-ses-contactlist` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un elenco di contatti di Amazon SES contiene tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se l'elenco dei contatti non ha alcuna chiave tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se l'elenco dei contatti non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori

best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un elenco di contatti di Amazon SES, consulta TagResourceAmazon SES API v2 Reference.

[SES.2] I set di configurazione SES devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::SES::ConfigurationSet`

AWS Configregola: `tagged-ses-configurationset` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS.	Nessun valore predefinito

Questo controllo verifica se un set di configurazione Amazon SES contiene tag con le chiavi specifiche definite nel parametro`requiredTagKeys`. Il controllo fallisce se il set di configurazione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una

chiave di tag e fallisce se il set di configurazione non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a moltiServizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un set di configurazione Amazon SES, consulta TagResourceAmazon SES API v2 Reference.

[SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::SES::ConfigurationSet`

Regola AWS Config: ses-sending-tls-required

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un set di configurazione Amazon SES richiede connessioni TLS. Il controllo fallisce se la politica TLS non è impostata su `'REQUIRE'` per un set di configurazione.

Per impostazione predefinita, Amazon SES utilizza il TLS opportunistico, il che significa che le e-mail possono essere inviate in modo non crittografato se non è possibile stabilire una connessione TLS con il server di posta ricevente. L'applicazione del TLS per l'invio di e-mail garantisce che i messaggi vengano recapitati solo quando è possibile stabilire una connessione crittografata sicura. Questo aiuta a proteggere la riservatezza e l'integrità dei contenuti e-mail durante la trasmissione tra Amazon SES e il server di posta del destinatario. Se non è possibile stabilire una connessione TLS sicura, il messaggio non verrà recapitato, evitando la potenziale esposizione di informazioni sensibili.

> **Note**
>
> Sebbene TLS 1.3 sia il metodo di consegna predefinito per Amazon SES, senza imporre i requisiti TLS tramite set di configurazione, i messaggi potrebbero essere recapitati in testo semplice se una connessione TLS fallisce. Per passare questo controllo, è necessario configurare la politica TLS `'REQUIRE'` nelle opzioni di consegna del set di configurazione SES. Quando è richiesto TLS, i messaggi vengono recapitati solo se è possibile stabilire una connessione TLS con il server di posta ricevente.

Correzione

Per configurare Amazon SES in modo che richieda connessioni TLS per un set di configurazione, consulta Amazon SES e i protocolli di sicurezza nella Amazon SES Developer Guide.

Controlli CSPM del Security Hub per Amazon SNS

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon Simple Notification Service (Amazon SNS). I controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[SNS.1] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS

Requisiti correlati: 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), NIST.800-171.r2 3.13.11, 3.13.16, CRI Profile NIST.800-171.r2 v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::SNS::Topic`

Regola AWS Config : `sns-encrypted-kms`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un argomento Amazon SNS è crittografato quando è inattivo utilizzando chiavi gestite in AWS Key Management Service ()AWS KMS. I controlli falliscono se l'argomento SNS non utilizza una chiave KMS per la crittografia lato server (SSE). Per impostazione predefinita, SNS archivia messaggi e file utilizzando la crittografia del disco. Per passare questo controllo, devi invece scegliere di utilizzare una chiave KMS per la crittografia. Ciò aggiunge un ulteriore livello di sicurezza e offre una maggiore flessibilità nel controllo degli accessi.

La crittografia dei dati inattivi riduce il rischio di accesso ai dati archiviati su disco da parte di un utente non autenticato. AWS Le autorizzazioni API sono necessarie per decrittografare i dati prima che possano essere letti. Ti consigliamo di crittografare gli argomenti SNS con chiavi KMS per un ulteriore livello di sicurezza.

Correzione

Per abilitare SSE per un argomento SNS, consulta Enabling server-side encryption (SSE) per un argomento Amazon SNS nella Amazon Simple Notification Service Developer Guide. Prima di poter utilizzare SSE, devi anche configurare AWS KMS key le politiche per consentire la crittografia degli argomenti e la crittografia e la decrittografia dei messaggi. Per ulteriori informazioni, consulta Configurazione delle AWS KMS autorizzazioni nella Guida per gli sviluppatori di Amazon Simple Notification Service.

[SNS.3] Gli argomenti SNS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::SNS::Topic`

AWS Config regola: `tagged-sns-topic` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un argomento di Amazon SNS contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'argomento non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'argomento non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un argomento SNS, consulta Configurazione dei tag degli argomenti di Amazon SNS nella Amazon Simple Notification Service Developer Guide.

[SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico

Requisiti correlati: CRI Profile v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Severità: critica

Tipo di risorsa: `AWS::SNS::Topic`

Regola AWS Config : sns-topic-no-public-access

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la policy di accesso agli argomenti di Amazon SNS consente l'accesso pubblico. Questo controllo fallisce se la policy di accesso agli argomenti di SNS consente l'accesso pubblico.

Utilizzi una policy di accesso di Amazon SNS con un argomento particolare per limitare chi può lavorare su quell'argomento (ad esempio, chi può pubblicare messaggi sull'argomento o chi può abbonarsi). Le policy SNS possono concedere l'accesso ad altri Account AWS utenti o a utenti interni al tuo. Account AWS L'immissione di una jolly (*) nel `Principal` campo della policy tematica e la mancanza di condizioni che limitino tale policy può comportare l'esfiltrazione dei dati, l'interruzione del servizio o l'inserimento indesiderato di messaggi nel servizio da parte di un utente malintenzionato.

> **Note**
>
> Questo controllo non valuta le condizioni delle policy che utilizzano caratteri jolly o variabili. Per produrre un `PASSED` risultato, le condizioni nella politica di accesso di Amazon SNS per

un argomento devono utilizzare solo valori fissi, ovvero valori che non contengono caratteri jolly o variabili di policy. Per informazioni sulle variabili di policy, consulta Variabili e tag nella Guida per l'AWS Identity and Access Management utente.

Correzione

Per aggiornare le politiche di accesso per un argomento SNS, consulta Overview of management access in Amazon SNS nella Amazon Simple Notification Service Developer Guide.

Controlli CSPM del Security Hub per Amazon SQS

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse Amazon Simple Queue Service (Amazon SQS). I controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive

Requisiti correlati: 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), (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::SQS::Queue`

AWS Config regola: `sqs-queue-encrypted` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una coda Amazon SQS è crittografata quando è inattiva. Il controllo fallisce se la coda non è crittografata con una SQS-managed chiave (SSE-SQS) o una chiave AWS Key Management Service (AWS KMS) (). SSE-KMS

La crittografia dei dati inattivi riduce il rischio che un utente non autorizzato acceda ai dati archiviati su disco. Server-side la crittografia (SSE) protegge il contenuto dei messaggi nelle code SQS utilizzando chiavi di SQS-managed crittografia () o chiavi (SSE-SQS). AWS KMS SSE-KMS

Correzione

Per configurare SSE per una coda SQS, consulta Configurazione della crittografia lato server (SSE) per una coda (console) nella Amazon Simple Queue Service Developer Guide.

[] Le code SQS devono essere etichettate SQS.2

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::SQS::Queue`

AWS Config regola: `tagged-sqs-queue` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se una coda Amazon SQS ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la coda non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la coda non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse.

L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice sull'etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una coda esistente utilizzando la console Amazon SQS, consulta Configuring cost allocation tags for a Amazon SQS queue (console) nella Amazon Simple Queue Service Developer Guide.

[SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico

Requisiti correlati: CRI Profile v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. IR-01.01, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Gestione sicura degli accessi > Risorsa non accessibile al pubblico

Severità: critica

Tipo di risorsa: `AWS::SQS::Queue`

Regola AWS Config : sqs-queue-no-public-access

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una policy di accesso di Amazon SQS consente l'accesso pubblico a una coda SQS. Il controllo fallisce se una policy di accesso SQS consente l'accesso pubblico alla coda.

Una policy di accesso di Amazon SQS può consentire l'accesso pubblico a una coda SQS, il che potrebbe consentire a un utente anonimo o a qualsiasi identità AWS IAM autenticata di accedere alla coda. Le policy di accesso SQS in genere forniscono questo accesso specificando il carattere jolly (*) nell'`Principal`elemento della policy, non utilizzando condizioni adeguate per limitare l'accesso alla coda, o entrambe le cose. Se una politica di accesso SQS consente l'accesso pubblico, terze parti potrebbero essere in grado di eseguire attività come ricevere messaggi dalla coda, inviare messaggi alla coda o modificare la politica di accesso per la coda. Ciò potrebbe causare eventi come l'esfiltrazione di dati, l'interruzione del servizio o l'inserimento di messaggi nella coda da parte di un autore della minaccia.

> **Note**
>
> Questo controllo non valuta le condizioni delle policy che utilizzano caratteri jolly o variabili. Per produrre un `PASSED` risultato, le condizioni nella policy di accesso di Amazon SQS per una coda devono utilizzare solo valori fissi, ossia valori che non contengono caratteri jolly o variabili di policy. Per informazioni sulle variabili di policy, consulta Variabili e tag nella Guida per l'AWS Identity and Access Management utente.

Correzione

Per informazioni sulla configurazione della policy di accesso SQS per una coda SQS, consulta Using custom policies with the Amazon SQS Access Policy Language nella Amazon Simple Queue Service Developer Guide.

Controlli CSPM Security Hub per Step Functions

Questi AWS Security Hub CSPM controlli valutano il AWS Step Functions servizio e le risorse.

Questi controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata

Requisiti correlati: PCI DSS v4.0. 1/10.4.2, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::StepFunctions::StateMachine`

Regola AWS Config : `step-functions-state-machine-logging-enabled`

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`logLevel`	Livello minimo di registrazione	Enum	`ALL`, `ERROR`, `FATAL`	Nessun valore predefinito

Questo controlla se una macchina a AWS Step Functions stati ha la registrazione attivata. Il controllo fallisce se una macchina a stati non ha la registrazione attivata. Se si fornisce un valore personalizzato per il `logLevel` parametro, il controllo viene eseguito solo se sulla macchina a stati è attivato il livello di registrazione specificato.

Il monitoraggio aiuta a mantenere l'affidabilità, la disponibilità e le prestazioni di Step Functions. È necessario raccogliere tutti i dati di monitoraggio Servizi AWS che si utilizzano in modo da poter eseguire più facilmente il debug degli errori multipunto. Avere una configurazione di registrazione definita per le tue macchine a stati Step Functions ti consente di tenere traccia della cronologia di esecuzione e dei risultati in Amazon CloudWatch Logs. Facoltativamente, puoi tenere traccia solo degli errori o degli eventi fatali.

Correzione

Per attivare la registrazione per una macchina a stati Step Functions, consulta Configure logging nella AWS Step Functions Developer Guide.

[StepFunctions.2] Le attività di Step Functions devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::StepFunctions::Activity`

AWS Config regola: `tagged-stepfunctions-activity` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un' AWS Step Functions attività ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'attività non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'attività non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'attività di Step Functions, consulta Tagging in Step Functions nella AWS Step Functions Developer Guide.

Controlli CSPM di Security Hub per Systems Manager

Questi AWS Security Hub CSPM controlli valutano il servizio e le risorse AWS Systems Manager (SSM). I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[SSM.1] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager

Requisiti correlati: 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), (1) NIST.800-53.r5 CM-8, 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, profilo CRI v2. 2/PR. PS-01.01

Categoria: Identificazione > Inventario

Gravità: media

Risorsa valutata: `AWS::EC2::Instance`

Risorse AWS Config di registrazione richieste:`AWS::EC2::Instance`, `AWS::SSM::ManagedInstanceInventory`

Regola AWS Config : ec2-instance-managed-by-systems-manager

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le istanze EC2 interrotte e in esecuzione nel tuo account sono gestite da. AWS Systems Manager Systems Manager è uno Servizio AWS strumento che puoi utilizzare per visualizzare e controllare la tua AWS infrastruttura.

Per aiutarti a mantenere la sicurezza e la conformità, Systems Manager analizza le istanze gestite interrotte e in esecuzione. Un'istanza gestita è una macchina configurata per l'uso con Systems Manager. Systems Manager segnala quindi o intraprende azioni correttive in caso di violazioni delle policy rilevate. Systems Manager consente inoltre di configurare e mantenere le istanze gestite. Per ulteriori informazioni, consulta la Guida per l'utente di AWS Systems Manager.

> **Note**
>
> Questo controllo genera `FAILED` risultati per le istanze EC2 che sono istanze di AWS Elastic Disaster Recovery Replication Server gestite da. AWS Un'istanza Replication Server è un'istanza EC2 che viene avviata automaticamente AWS Elastic Disaster Recovery per supportare la replica continua dei dati dai server di origine. AWS rimuove intenzionalmente l'agente Systems Manager (SSM) da queste istanze per mantenere l'isolamento e aiutare a prevenire potenziali percorsi di accesso non intenzionali.

Correzione

Per informazioni sulla gestione delle istanze EC2 con AWS Systems Manager, consulta la gestione degli host di Amazon EC2 nella AWS Systems Manager Guida per l'utente. Nella sezione Opzioni di configurazione della AWS Systems Manager console, puoi mantenere le impostazioni predefinite o modificarle secondo necessità per la tua configurazione preferita.

[SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch

Requisiti correlati: 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. 1/6.2, PCI DSS versione 4.0. 1/2.2.1, PCI DSS versione 4.0. 1/6.3.3, Profilo CRI v2. 2/ID. RA-01.03, Profilo CRI v2. 2/PR. PS-02.01

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: `AWS::SSM::PatchCompliance`

Regola AWS Config : ec2-managedinstance-patch-compliance-status-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se lo stato di conformità della patch di Systems Manager è `COMPLIANT` o `NON_COMPLIANT` dopo l'installazione della patch sull'istanza. Il controllo ha esito negativo se lo stato di conformità è`NON_COMPLIANT`. Il controllo controlla solo le istanze gestite da Systems Manager Patch Manager.

L'applicazione di patch alle istanze EC2 come richiesto dall'organizzazione riduce la superficie di attacco della vostra. Account AWS

Correzione

Systems Manager consiglia di utilizzare le policy di patch per configurare l'applicazione delle patch per le istanze gestite. È inoltre possibile utilizzare i documenti Systems Manager, come descritto nella procedura seguente, per applicare patch a un'istanza.

Per correggere le patch non conformi

1. Aprire la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Per Gestione dei nodi, scegli Esegui comando, quindi scegli Esegui comando.
3. Scegli l'opzione per AWS- RunPatchBaseline.
4. Modificare l'operazione su Install (Installa).
5. Scegli le istanze manualmente, quindi scegli le istanze non conformi.
6. Scegli Esegui.
7. Una volta completato il comando, per monitorare il nuovo stato di conformità delle istanze a cui è stata applicata la patch, scegli Conformità nel riquadro di navigazione.

[SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), (1) NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SI-2 PCI DSS v3.2. 1/2.4, PCI DSS versione 4.0. 1/2.2.1, PCI DSS versione 4.0. 1/6.3.3, Profilo CRI v2. 2/

DE. CM-01.03, Profilo CRI v2. 2/DE. CM-09.03, Profilo CRI v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-02.01, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. IR-01.03, Profilo CRI v2. 2/PR. IR-01.05

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa: `AWS::SSM::AssociationCompliance`

Regola AWS Config : ec2-managedinstance-association-compliance-status-check

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se lo stato della conformità dell' AWS Systems Manager associazione è `COMPLIANT` o `NON_COMPLIANT` dopo l'esecuzione dell'associazione su un'istanza. Il controllo ha esito negativo se lo stato di conformità dell'associazione è`NON_COMPLIANT`.

Un'associazione State Manager è una configurazione assegnata alle istanze gestite. La configurazione definisce lo stato che desideri mantenere sulle istanze. Ad esempio, un'associazione può specificare che il software antivirus deve essere installato e in esecuzione sulle istanze o che determinate porte devono essere chiuse.

Dopo aver creato una o più associazioni di State Manager, le informazioni sullo stato di conformità sono immediatamente disponibili. È possibile visualizzare lo stato di conformità nella console o in risposta ai AWS CLI comandi o alle azioni API Systems Manager corrispondenti. Per le associazioni, Configuration Compliance mostra lo stato di conformità (`Compliant`o`Non-compliant`). Mostra anche il livello di gravità assegnato all'associazione, ad esempio `Critical` o`Medium`.

Per ulteriori informazioni sulla conformità dell'associazione State Manager, vedere Informazioni sulla conformità all'associazione State Manager nella Guida per l'AWS Systems Manager utente.

Correzione

Un'associazione fallita può essere correlata a diversi fattori, tra cui destinazioni e nomi di documenti Systems Manager. Per risolvere questo problema, è necessario innanzitutto identificare e analizzare l'associazione visualizzando la cronologia delle associazioni. Per istruzioni sulla visualizzazione della cronologia delle associazioni, vedere Visualizzazione della cronologia delle associazioni nella Guida per l'AWS Systems Manager utente.

Dopo aver esaminato, è possibile modificare l'associazione per correggere il problema identificato. Puoi modificare un'associazione per specificare un nome, una pianificazione, un livello di gravità o target nuovi. Dopo aver modificato un'associazione, AWS Systems Manager crea una nuova versione. Per istruzioni sulla modifica di un'associazione, consulta Modifica e creazione di una nuova versione di un'associazione nella Guida per l'AWS Systems Manager utente.

[SSM.4] I documenti SSM non devono essere pubblici

Requisiti correlati: 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 Profile v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. IR-01.01

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Severità: critica

Tipo di risorsa: `AWS::SSM::Document`

Regola AWS Config : ssm-document-not-public

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se AWS Systems Manager i documenti di proprietà di un account sono pubblici. Il controllo fallisce se i documenti di Systems Manager che hanno `Self` come proprietario sono pubblici.

I documenti pubblici di Systems Manager potrebbero consentire l'accesso non intenzionale ai documenti. Un documento pubblico di Systems Manager può esporre informazioni preziose sull'account, sulle risorse e sui processi interni.

A meno che il tuo caso d'uso non richieda la condivisione pubblica, ti consigliamo di bloccare la condivisione pubblica per i documenti di Systems Manager che hai `Self` come proprietario.

Correzione

Per informazioni sulla configurazione della condivisione per i documenti di Systems Manager, vedere Condividi un documento SSM nella Guida per l'AWS Systems Manager utente.

[SSM.5] I documenti SSM devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::SSM::Document`

Regola AWS Config : ssm-document-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un AWS Systems Manager documento ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo ha esito negativo se il documento non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il documento non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso. Il controllo non valuta i documenti Systems Manager di proprietà di Amazon.

Un tag è un'etichetta che crei e assegni a una AWS risorsa. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli

accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per aggiungere tag a un AWS Systems Manager documento, puoi utilizzare il AddTagsToResourcefunzionamento dell' AWS Systems Manager API o, se utilizzi il AWS CLI, eseguire il comando add-tags-to-resource. Puoi anche utilizzare la console AWS Systems Manager .

[SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch

Requisiti correlati: CRI Profile v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : ssm-automation-logging-enabled

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la CloudWatch registrazione di Amazon è abilitata per l'automazione AWS Systems Manager (SSM). Il controllo fallisce se la CloudWatch registrazione non è abilitata per SSM Automation.

SSM Automation è uno AWS Systems Manager strumento che ti aiuta a creare soluzioni automatizzate per distribuire, configurare e gestire AWS risorse su larga scala utilizzando runbook

predefiniti o personalizzati. Per soddisfare i requisiti operativi o di sicurezza dell'organizzazione, potrebbe essere necessario fornire un registro degli script eseguiti. Puoi configurare SSM Automation per inviare l'output `aws:executeScript` delle azioni nei tuoi runbook a un gruppo di log Amazon CloudWatch Logs da te specificato. Con CloudWatch Logs, puoi monitorare, archiviare e accedere a file di registro da diversi file. Servizi AWS

Correzione

Per informazioni sull'abilitazione della CloudWatch registrazione per SSM Automation, consulta l'output dell'azione Logging Automation with CloudWatch Logs nella Guida per l'utente.AWS Systems Manager

[SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata

Requisiti correlati: CRI Profile v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. AA-01.02, Profilo CRI v2. 2/PR. AA-03.02, Profilo CRI v2. 2/PR. AA-05.01, Profilo CRI v2. 2/PR. PS-01.01, Profilo CRI v2. 2/PR. PS-01.02

Categoria: Protezione > Gestione sicura degli accessi > Risorsa non accessibile al pubblico

Severità: critica

Tipo di risorsa: `AWS::::Account`

Regola AWS Config : ssm-automation-block-public-sharing

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se l'impostazione di blocco della condivisione pubblica è abilitata per AWS Systems Manager i documenti. Il controllo fallisce se l'impostazione di blocco della condivisione pubblica è disabilitata per i documenti di Systems Manager.

L'impostazione di condivisione pubblica a blocchi per i documenti AWS Systems Manager (SSM) è un'impostazione a livello di account. L'attivazione di questa impostazione può impedire l'accesso indesiderato ai documenti SSM. Se abiliti questa impostazione, la modifica non influirà sui documenti SSM che stai attualmente condividendo con il pubblico. A meno che il tuo caso d'uso non richieda la condivisione di documenti SSM con il pubblico, ti consigliamo di abilitare l'impostazione di blocco della condivisione pubblica. L'impostazione può essere diversa per ognuno di essi Regione AWS.

Correzione

Per informazioni sull'attivazione dell'impostazione di blocco della condivisione pubblica per i documenti AWS Systems Manager (SSM), consulta Bloccare la condivisione pubblica per i documenti SSM nella Guida per l'AWS Systems Manager utente.

Controlli CSPM Security Hub per AWS Transfer Family

Questi AWS Security Hub CSPM controlli valutano il AWS Transfer Family servizio e le risorse. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[Transfer.1] AWS Transfer Family i flussi di lavoro devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Transfer::Workflow`

AWS Config regola: `tagged-transfer-workflow` (regola CSPM Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredTagKeys`	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	`No default value`

Questo controllo verifica se un AWS Transfer Family flusso di lavoro ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo ha esito negativo se il flusso di lavoro non ha

alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro`requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il flusso di lavoro non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con`aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

> **Note**
>
> Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un flusso di lavoro Transfer Family (console)

1. Apri la AWS Transfer Family console.
2. Nel pannello di navigazione, scegli Workflows (Flussi di lavoro). Quindi, seleziona il flusso di lavoro a cui desideri taggare.
3. Scegli Gestisci tag, quindi aggiungi i tag.

[Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint

Requisiti correlati: 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, Profilo CRI v2. 2/PR. DS-02.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: `AWS::Transfer::Server`

Regola AWS Config : transfer-family-server-no-ftp

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un AWS Transfer Family server utilizza un protocollo diverso dall'FTP per la connessione agli endpoint. Il controllo fallisce se il server utilizza il protocollo FTP per consentire a un client di connettersi all'endpoint del server.

L'FTP (File Transfer Protocol) stabilisce la connessione all'endpoint tramite canali non crittografati, rendendo i dati inviati su questi canali vulnerabili all'intercettazione. L'utilizzo di SFTP (SSH File Transfer Protocol), FTPS (File Transfer Protocol Secure) o AS2 (Applicability Statement 2) offre un ulteriore livello di sicurezza crittografando i dati in transito e può essere utilizzato per impedire a potenziali aggressori di utilizzare attacchi person-in-the-middle o attacchi simili per intercettare o manipolare il traffico di rete.

Correzione

Per modificare il protocollo per un server Transfer Family, vedere Modifica i protocolli di trasferimento dei file nella Guida per l'AWS Transfer Family utente.

[Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata

Requisiti correlati: 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), (8), NIST.800-53.r5 SI-3 (20) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), CRI Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/DE. AE-03.02, Profilo CRI v2. 2/DE. CM-03.01, Profilo CRI v2. 2/DE. CM-03.02, Profilo CRI v2. 2/DE. CM-03.03, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::Transfer::Connector`

Regola AWS Config : transfer-connector-logging-enabled

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la CloudWatch registrazione di Amazon è abilitata per un AWS Transfer Family connettore. Il controllo fallisce se CloudWatch la registrazione non è abilitata per il connettore.

Amazon CloudWatch è un servizio di monitoraggio e osservabilità che offre visibilità sulle tue AWS risorse, comprese le AWS Transfer Family risorse. Per Transfer Family, CloudWatch fornisce un controllo e una registrazione consolidati per l'avanzamento e i risultati del flusso di lavoro. Ciò include diverse metriche che Transfer Family definisce per i flussi di lavoro. È possibile configurare Transfer Family per registrare automaticamente gli eventi del connettore CloudWatch. A tale scopo, è necessario specificare un ruolo di registrazione per il connettore. Per il ruolo di registrazione, crei un ruolo IAM e una policy IAM basata sulle risorse che definisce le autorizzazioni per il ruolo.

Correzione

Per informazioni sull'abilitazione della CloudWatch registrazione per un connettore Transfer Family, consulta Amazon CloudWatch logging for AWS Transfer Family servers nella AWS Transfer Family User Guide.

[Transfer.4] Gli accordi Transfer Family devono essere etichettati

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Transfer::Agreement`

Regola AWS Config : transfer-agreement-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un AWS Transfer Family accordo ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo ha esito negativo se l'accordo non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'accordo non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un AWS Transfer Family accordo, consulta Metodi di etichettatura delle risorse nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

[Transfer.5] I certificati Transfer Family devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Transfer::Certificate`

Regola AWS Config : transfer-certificate-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un AWS Transfer Family certificato ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo ha esito negativo se il certificato non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il certificato non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le

risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un AWS Transfer Family certificato, consulta Metodi di etichettatura delle risorse nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

[Transfer.6] I connettori Transfer Family devono essere etichettati

Requisiti correlati: CRI Profile v2. 2/ID. AM-02.01, Profilo CRI v2. 2/ID. AM-05.01

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Transfer::Connector`

Regola AWS Config : transfer-connector-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un AWS Transfer Family connettore ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo ha esito negativo se il connettore non ha alcuna chiave tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il connettore non dispone di chiavi di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso.

Un tag è un'etichetta che si crea e si assegna a una risorsa. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un AWS Transfer Family connettore, consulta Metodi di etichettatura delle risorse nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

[Transfer.7] I profili Transfer Family devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Transfer::Profile`

Regola AWS Config : transfer-profile-tagged

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Description	Tipo	Valori personalizzati consentiti	Valore predefinito CSPM di Security Hub
`requiredKeyTags`	Un elenco di chiavi di tag non di sistema che devono essere assegnate a una risorsa valutata. I tag fanno distinzione tra maiuscole e minuscole	StringList (massimo 6 articoli)	1—6 tasti tag che soddisfano i requisiti AWS .	Nessun valore predefinito

Questo controllo verifica se un AWS Transfer Family profilo ha le chiavi dei tag specificate dal `requiredKeyTags` parametro. Il controllo ha esito negativo se il profilo non ha alcuna chiave di tag o non ha tutte le chiavi specificate dal `requiredKeyTags` parametro. Se non specificate alcun valore per il `requiredKeyTags` parametro, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il profilo non ha alcuna chiave di tag. Il controllo ignora i tag di sistema, che vengono applicati automaticamente e hanno il `aws:` prefisso. Il controllo valuta i profili locali e i profili dei partner.

Un tag è un'etichetta che crei e assegni a una AWS risorsa. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag facoltativo. È possibile utilizzare i tag per classificare le

risorse in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. Possono anche aiutarti a tenere traccia delle azioni e delle notifiche dei proprietari delle risorse. Puoi anche utilizzare i tag per implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione. Per ulteriori informazioni sulle strategie ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC nella IAM User Guide. Per ulteriori informazioni sui tag, consulta la Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. I tag sono accessibili da molti Servizi AWS. Non sono destinati a essere utilizzati per dati privati o sensibili.

Correzione

Per informazioni sull'aggiunta di tag a un AWS Transfer Family profilo, consulta Metodi di etichettatura delle risorse nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

Controlli CSPM Security Hub per AWS WAF

Questi AWS Security Hub CSPM controlli valutano il AWS WAF servizio e le risorse. I controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata

Requisiti correlati: 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), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. PS-04.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::WAF::WebACL`

Regola AWS Config : `waf-classic-logging-enabled`

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la registrazione è abilitata per un ACL web AWS WAF globale. Questo controllo ha esito negativo se la registrazione non è abilitata per l'ACL Web.

La registrazione è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni a livello globale. AWS WAF È un requisito aziendale e di conformità in molte organizzazioni e consente di risolvere i problemi relativi al comportamento delle applicazioni. Fornisce inoltre informazioni dettagliate sul traffico analizzato dall'ACL Web a cui è allegato. AWS WAF

Correzione

Per abilitare la registrazione per un ACL AWS WAF Web, consulta la sezione Registrazione delle informazioni sul traffico ACL Web nella Developer Guide.AWS WAF

[WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione

Requisiti correlati: 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 Profile v2. 2/DE. CM-01.01, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.02

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: `AWS::WAFRegional::Rule`

Regola AWS Config : `waf-regional-rule-not-empty`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una regola AWS WAF regionale ha almeno una condizione. Il controllo ha esito negativo se non sono presenti condizioni all'interno di una regola.

Una regola regionale WAF può contenere più condizioni. Le condizioni della regola consentono l'ispezione del traffico e l'esecuzione di un'azione definita (consentire, bloccare o contare). Senza

alcuna condizione, il traffico scorre senza ispezioni. Una regola regionale WAF priva di condizioni, ma con un nome o tag che suggerisca di consentire, bloccare o contare, potrebbe indurre a supporre erroneamente che una di queste azioni si stia verificando.

Correzione

Per aggiungere una condizione a una regola vuota, consulta Aggiungere e rimuovere condizioni in una regola nella Guida per gli sviluppatori.AWS WAF

[WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola

Requisiti correlati: 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 Profile v2. 2/DE. CM-01.01, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.02

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: `AWS::WAFRegional::RuleGroup`

Regola AWS Config : `waf-regional-rulegroup-not-empty`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo di regole AWS WAF regionali ha almeno una regola. Il controllo ha esito negativo se non è presente alcuna regola all'interno di un gruppo di regole.

Un gruppo di regole regionali WAF può contenere più regole. Le condizioni della regola consentono l'ispezione del traffico e l'esecuzione di un'azione definita (consentire, bloccare o contare). Senza regole, il traffico scorre senza ispezioni. Un gruppo di regole regionali WAF privo di regole, ma con un nome o un tag che suggerisce l'autorizzazione, il blocco o il numero, potrebbe indurre a supporre erroneamente che una di queste azioni sia in corso.

Correzione

Per aggiungere regole e condizioni di regole a un gruppo di regole vuoto, consulta Aggiungere ed eliminare regole da un gruppo di regole AWS WAF classico e Aggiungere e rimuovere condizioni in una regola nella Guida per gli sviluppatori.AWS WAF

[WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/DE. CM-01.01, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.02

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: `AWS::WAFRegional::WebACL`

Regola AWS Config : `waf-regional-webacl-not-empty`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un ACL AWS WAF Classic regionale Web contiene regole WAF o gruppi di regole WAF. Questo controllo ha esito negativo se un ACL Web non contiene regole o gruppi di regole WAF.

Un ACL web WAF regionale può contenere una raccolta di regole e gruppi di regole che esaminano e controllano le richieste web. Se un ACL web è vuoto, il traffico web può passare senza essere rilevato o modificato da WAF, a seconda dell'azione predefinita.

Correzione

Per aggiungere regole o gruppi di regole a un ACL web regionale AWS WAF classico vuoto, consulta Modifica di un ACL Web nella Guida per gli sviluppatori.AWS WAF

[WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/DE. CM-01.01, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.02

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: `AWS::WAF::Rule`

Regola AWS Config : `waf-global-rule-not-empty`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una regola AWS WAF globale contiene condizioni. Il controllo ha esito negativo se non sono presenti condizioni all'interno di una regola.

Una regola globale WAF può contenere più condizioni. Le condizioni di una regola consentono l'ispezione del traffico e l'esecuzione di un'azione definita (consentire, bloccare o contare). Senza alcuna condizione, il traffico scorre senza ispezioni. Una regola globale WAF priva di condizioni, ma con un nome o tag che suggerisca di consentire, bloccare o contare, potrebbe portare a supporre erroneamente che una di queste azioni sia in corso.

Correzione

Per istruzioni sulla creazione di una regola e sull'aggiunta di condizioni, consulta Creazione di una regola e aggiunta di condizioni nella Guida per gli sviluppatori.AWS WAF

[WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/DE. CM-01.01, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.03

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: `AWS::WAF::RuleGroup`

Regola AWS Config : `waf-global-rulegroup-not-empty`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo di regole AWS WAF globale ha almeno una regola. Il controllo ha esito negativo se non è presente alcuna regola all'interno di un gruppo di regole.

Un gruppo di regole globale WAF può contenere più regole. Le condizioni della regola consentono l'ispezione del traffico e l'esecuzione di un'azione definita (consentire, bloccare o contare). Senza regole, il traffico scorre senza ispezioni. Un gruppo di regole globale WAF senza regole, ma con un nome o un tag che suggerisce di consentire, bloccare o contare, potrebbe portare a supporre erroneamente che una di queste azioni sia in corso.

Correzione

Per istruzioni sull'aggiunta di una regola a un gruppo di regole, consulta Creating an AWS WAF Classic rule group nella Developer Guide.AWS WAF

[WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Requisiti correlati: 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 Profile v2. 2/DE. CM-01.01, Profilo CRI v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.02

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: `AWS::WAF::WebACL`

Regola AWS Config : `waf-global-webacl-not-empty`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un ACL web AWS WAF globale contiene almeno una regola WAF o un gruppo di regole WAF. Il controllo ha esito negativo se un ACL Web non contiene regole o gruppi di regole WAF.

Un ACL web globale WAF può contenere una raccolta di regole e gruppi di regole che esaminano e controllano le richieste web. Se un ACL Web è vuoto, il traffico Web può passare senza essere rilevato o modificato da WAF, a seconda dell'azione predefinita.

Correzione

Per aggiungere regole o gruppi di regole a un ACL web AWS WAF globale vuoto, consulta Modifica di un ACL web nella Guida per gli sviluppatori.AWS WAF Per Filtro, scegliete Globale () CloudFront.

[WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole

Requisiti correlati: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, CRI Profile v2. 2/DE. CM-01.03, Profilo CRI v2. 2/PR. IR-01.02, Profilo CRI v2. 2/PR. PS-01.01

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: `AWS::WAFv2::WebACL`

Regola AWS Config : `wafv2-webacl-not-empty`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un elenco di controllo degli accessi Web AWS WAF V2 (Web ACL) contiene almeno una regola o un gruppo di regole. Il controllo ha esito negativo se un ACL Web non contiene regole o gruppi di regole.

Un ACL Web offre un controllo dettagliato su tutte le richieste Web HTTP (S) a cui risponde la risorsa protetta. Un ACL Web deve contenere una raccolta di regole e gruppi di regole che esaminano e controllano le richieste Web. Se un ACL Web è vuoto, il traffico Web può passare senza essere rilevato o modificato, AWS WAF a seconda dell'azione predefinita.

Correzione

Per aggiungere regole o gruppi di regole a un ACL web WAFV2 vuoto, vedere Modifica di un ACL Web nella Guida per gli sviluppatori.AWS WAF

[WAF.11] AWS WAF la registrazione ACL web deve essere abilitata

Requisiti correlati: 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), (10) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/PR. PS-04.01, Profilo CRI v2. 2/PR. PS-04.02, Profilo CRI v2. 2/PR. PS-04.03

Categoria: Identificazione > Registrazione

Gravità: bassa

Tipo di risorsa: `AWS::WAFv2::WebACL`

AWS Config regola: **`wafv2-logging-enabled`**

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la registrazione è attivata per un elenco di controllo degli accessi Web AWS WAF V2 (Web ACL). Questo controllo ha esito negativo se la registrazione è disattivata per l'ACL Web.

> **Note**
>
> Questo controllo non verifica se la registrazione AWS WAF Web ACL è abilitata per un account tramite Amazon Security Lake.

La registrazione mantiene l'affidabilità, la disponibilità e le prestazioni di. AWS WAF Inoltre, la registrazione è un requisito aziendale e di conformità in molte organizzazioni. Registrando il traffico analizzato dall'ACL Web, è possibile risolvere i problemi relativi al comportamento delle applicazioni.

Correzione

Per attivare la registrazione per un ACL AWS WAF Web, consulta Managing logging for a Web ACL nella Developer Guide.AWS WAF

[WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch

Requisiti correlati: 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), (10) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-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 Profile v2. 2/DE. AE-02.01, Profilo CRI v2. 2/DE. AE-02.02, Profilo CRI v2. 2/DE. AE-03.01, Profilo CRI v2. 2/RS. MA-02.01

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::WAFv2::RuleGroup`

AWS Config regola: **`wafv2-rulegroup-logging-enabled`**

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una AWS WAF regola o un gruppo di regole ha i CloudWatch parametri Amazon abilitati. Il controllo fallisce se la regola o il gruppo di regole non ha le CloudWatch metriche abilitate.

La configurazione delle CloudWatch metriche su AWS WAF regole e gruppi di regole offre visibilità sul flusso di traffico. Puoi vedere quali regole ACL vengono attivate e quali richieste vengono accettate e bloccate. Questa visibilità può aiutarti a identificare attività dannose sulle risorse associate.

Correzione

Per abilitare le CloudWatch metriche su un gruppo di AWS WAF regole, richiama l' UpdateRuleGroupAPI. Per abilitare le CloudWatch metriche su una AWS WAF regola, richiama l'API ACL. UpdateWeb Imposta il campo su. `CloudWatchMetricsEnabled` `true` Quando utilizzi la AWS WAF console per creare regole o gruppi di regole, le CloudWatch metriche vengono abilitate automaticamente.

Controlli CSPM Security Hub per WorkSpaces

Questi AWS Security Hub CSPM controlli valutano il WorkSpaces servizio e le risorse Amazon.

Questi controlli potrebbero non essere disponibili tutti Regioni AWS. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

[WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi

Requisiti correlati: CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::WorkSpaces::Workspace`

Regola AWS Config : `workspaces-user-volume-encryption-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un volume utente in Amazon WorkSpaces WorkSpace è crittografato quando è inattivo. Il controllo fallisce se il volume WorkSpace utente non è crittografato a riposo.

I dati inattivi si riferiscono ai dati archiviati in uno storage persistente e non volatile per qualsiasi durata. La crittografia dei dati inutilizzati consente di proteggerne la riservatezza, riducendo il rischio che un utente non autorizzato possa accedervi.

Correzione

Per crittografare un volume WorkSpaces utente, consulta Encrypt a WorkSpace nella Amazon WorkSpaces Administration Guide.

[WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Requisiti correlati: CRI Profile v2. 2/PR. DS-01.01, Profilo CRI v2. 2/PR. PS-01.06, Profilo CRI v2. 2/PR. PS-01.08

Categoria: Protezione > Protezione dei dati > Crittografia dei dati archiviati

Gravità: media

Tipo di risorsa: `AWS::WorkSpaces::Workspace`

Regola AWS Config : `workspaces-root-volume-encryption-enabled`

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un volume root in Amazon WorkSpaces WorkSpace è crittografato a riposo. Il controllo fallisce se il volume WorkSpace root non è crittografato a riposo.

I dati inattivi si riferiscono ai dati archiviati in uno spazio di archiviazione persistente e non volatile per qualsiasi durata. La crittografia dei dati inutilizzati consente di proteggerne la riservatezza, riducendo il rischio che un utente non autorizzato possa accedervi.

Correzione

Per crittografare un volume WorkSpaces root, consulta Encrypt a WorkSpace nella Amazon WorkSpaces Administration Guide.

Autorizzazioni richieste per configurare i controlli in Security Hub CSPM

Per visualizzare informazioni sui controlli di sicurezza e abilitare e disabilitare i controlli di sicurezza negli standard, il ruolo AWS Identity and Access Management (IAM) utilizzato per accedere a AWS

Security Hub CSPM richiede le autorizzazioni per chiamare le seguenti operazioni dell'API CSPM di Security Hub.

Per ottenere le autorizzazioni necessarie, puoi utilizzare le politiche gestite da Security Hub CSPM. In alternativa, puoi aggiornare le policy IAM personalizzate per includere le autorizzazioni per queste azioni.

- BatchGetSecurityControls— Restituisce informazioni su una serie di controlli di sicurezza per l'account corrente eRegione AWS.
- ListSecurityControlDefinitions— Restituisce informazioni sui controlli di sicurezza che si applicano a uno standard specifico.
- ListStandardsControlAssociations— Indica se un controllo di sicurezza è attualmente abilitato o disabilitato in ogni standard abilitato nell'account.
- BatchGetStandardsControlAssociations— Per un batch di controlli di sicurezza, indica se ogni controllo è attualmente abilitato o disabilitato in base a uno standard specifico.
- BatchUpdateStandardsControlAssociations— Utilizzato per abilitare un controllo di sicurezza negli standard che includono il controllo o per disabilitare un controllo negli standard. Si tratta di un sostituto in batch dell'`UpdateStandardsControl`operazione esistente.
- BatchUpdateStandardsControlAssociations— Utilizzato per abilitare o disabilitare un batch di controlli di sicurezza negli standard che includono i controlli. Si tratta di un sostituto in batch dell'`UpdateStandardsControl`operazione esistente.
- UpdateStandardsControl— Utilizzato per abilitare o disabilitare un singolo controllo di sicurezza negli standard che includono il controllo
- DescribeStandardsControl— Restituisce dettagli sui controlli di sicurezza specifici.

Oltre alle API precedenti, è necessario aggiungere l'autorizzazione alla chiamata `BatchGetControlEvaluations` al proprio ruolo IAM. Questa autorizzazione è necessaria per visualizzare lo stato di attivazione e conformità di un controllo, i risultati contano per un controllo e il punteggio di sicurezza complessivo per i controlli sulla console CSPM di Security Hub. Poiché solo le chiamate alla console`BatchGetControlEvaluations`, questa autorizzazione non corrisponde direttamente alle API o ai comandi CSPM di Security Hub documentati pubblicamente. AWS CLI

Abilitazione dei controlli in Security Hub CSPM

In AWS Security Hub CSPM, un controllo è una protezione all'interno di uno standard di sicurezza che aiuta un'organizzazione a proteggere la riservatezza, l'integrità e la disponibilità delle proprie

informazioni. Ogni controllo CSPM di Security Hub è correlato a una risorsa specifica. AWS Quando si abilita un controllo, Security Hub CSPM inizia a eseguire i controlli di sicurezza per il controllo e ne genera i risultati. Security Hub CSPM considera inoltre tutti i controlli abilitati nel calcolo dei punteggi di sicurezza.

Puoi scegliere di abilitare un controllo per tutti gli standard di sicurezza a cui si applica. In alternativa, è possibile configurare lo stato di abilitazione in modo diverso nei diversi standard. Consigliamo la prima opzione, in cui lo stato di abilitazione di un controllo è allineato a tutti gli standard abilitati. Per istruzioni su come abilitare un controllo in tutti gli standard a cui viene applicato, consulta. Abilitare un controllo su tutti gli standard Per istruzioni su come abilitare un controllo in standard specifici, vedereAbilitazione di un controllo in uno standard specifico.

Se abiliti l'aggregazione tra regioni e accedi a una regione di aggregazione, la console Security Hub CSPM mostra i controlli disponibili in almeno una regione collegata. Se un controllo è disponibile in una regione collegata ma non nella regione di aggregazione, non puoi abilitare o disabilitare quel controllo dalla regione di aggregazione.

Puoi abilitare e disabilitare i controlli in ciascuna regione utilizzando la console Security Hub CSPM, l'API Security Hub CSPM o. AWS CLI

Le istruzioni per abilitare e disabilitare i controlli variano a seconda che si utilizzi o meno la configurazione centrale. ??? Questo argomento descrive le differenze. La configurazione centrale è disponibile per gli utenti che integrano Security Hub CSPM e. AWS Organizations Si consiglia di utilizzare la configurazione centrale per semplificare il processo di attivazione e disabilitazione dei controlli in ambienti con più account e più regioni. Se si utilizza la configurazione centrale, è possibile abilitare il controllo su più account e regioni tramite l'uso di politiche di configurazione. Se non utilizzi la configurazione centrale, devi abilitare un controllo separatamente in ogni regione e account.

Abilitare un controllo su tutti gli standard

Si consiglia di abilitare un controllo CSPM di AWS Security Hub per tutti gli standard a cui si applica il controllo. Se attivi i risultati di controllo consolidati, riceverai un risultato per controllo anche se un controllo appartiene a più di uno standard.

Cross-standard abilitazione in ambienti con più account e più regioni

Per abilitare un controllo di sicurezza su più aree Regioni AWS, è necessario accedere all'account amministratore CSPM di Security Hub delegato Account AWS e utilizzare la configurazione centrale. ???

In base alla configurazione centrale, l'amministratore delegato può creare politiche di configurazione CSPM di Security Hub che abilitano controlli specifici tra gli standard abilitati. È quindi possibile associare la politica di configurazione ad account e unità organizzative (OU) specifici o alla radice. Una politica di configurazione ha effetto nella tua regione di origine (chiamata anche regione di aggregazione) e in tutte le regioni collegate.

Le politiche di configurazione offrono la personalizzazione. Ad esempio, puoi scegliere di abilitare tutti i controlli in un'unità organizzativa e puoi scegliere di abilitare solo i controlli Amazon Elastic Compute Cloud (EC2) in un'altra unità organizzativa. Il livello di granularità dipende dagli obiettivi prefissati per la copertura di sicurezza nell'organizzazione. Per istruzioni sulla creazione di una politica di configurazione che abiliti controlli specifici tra gli standard, consulta. Creazione e associazione di policy di configurazione

> **Note**
>
> L'amministratore delegato può creare politiche di configurazione per gestire i controlli in tutti gli standard tranne lo Service-Managed Standard: AWS Control Tower. I controlli per questo standard devono essere configurati nel AWS Control Tower servizio.

Se si desidera che alcuni account configurino i propri controlli anziché l'amministratore delegato, l'amministratore delegato può designare tali account come autogestiti. Self-managed gli account devono configurare i controlli separatamente in ciascuna regione.

Cross-standard abilitazione in un unico account e regione

Se non utilizzi la configurazione centrale o sei un account autogestito, non puoi utilizzare le politiche di configurazione per abilitare centralmente i controlli in più account e regioni. Tuttavia, puoi utilizzare i seguenti passaggi per abilitare un controllo in un singolo account e regione.

Security Hub CSPM console

Per abilitare il controllo di tutti gli standard in un account e in un'area geografica

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Scegli Controlli dal pannello di navigazione.
3. Scegli la scheda Disabilitato.

4. Scegli l'opzione accanto a un controllo.
5. Scegli Abilita controllo (questa opzione non viene visualizzata per un controllo già abilitato).
6. Ripeti l'operazione in ogni regione in cui desideri abilitare il controllo.

Security Hub CSPM API

Per abilitare il controllo di tutti gli standard in un account e in una regione

1. Richiama l'ListStandardsControlAssociationsAPI. Fornisci un ID di controllo di sicurezza.

   Esempio di richiesta:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. Richiama l'BatchUpdateStandardsControlAssociationsAPI. Fornisci l'Amazon Resource Name (ARN) di tutti gli standard in cui il controllo non è abilitato. Per ottenere ARN standard, esegui. `DescribeStandards`
3. Imposta il `AssociationStatus` parametro uguale a. `ENABLED` Se segui questi passaggi per un controllo già abilitato, l'API restituisce una risposta con codice di stato HTTP 200.

   Esempio di richiesta:

   ```
   {
       "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. Ripetere l'operazione in ogni regione in cui si desidera abilitare il controllo.

AWS CLI

Per abilitare il controllo di tutti gli standard in un account e in una regione

1. Esegui il comando list-standards-control-associations. Fornisci un ID per il controllo di sicurezza.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Esegui il comando batch-update-standards-control-associations. Fornisci l'Amazon Resource Name (ARN) di tutti gli standard in cui il controllo non è abilitato. Per ottenere ARN standard, esegui il `describe-standards` comando.
3. Imposta il `AssociationStatus` parametro uguale a. `ENABLED` Se segui questi passaggi per un controllo già abilitato, il comando restituisce una risposta con codice di stato HTTP 200.

```
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. Ripetere l'operazione in ogni regione in cui si desidera abilitare il controllo.

Abilitazione di un controllo in uno standard specifico

Quando si abilita uno standard in AWS Security Hub CSPM, tutti i controlli ad esso applicabili vengono abilitati automaticamente in quello standard (ad eccezione degli standard gestiti dai servizi). È quindi possibile disabilitare e riattivare controlli specifici nello standard. Tuttavia, consigliamo di allineare lo stato di abilitazione di un controllo a tutti gli standard abilitati. Per istruzioni su come abilitare un controllo in tutti gli standard, consulta. Abilitare un controllo su tutti gli standard

La pagina dei dettagli di uno standard contiene l'elenco dei controlli applicabili allo standard e informazioni sui controlli attualmente abilitati e disattivati in tale standard.

Nella pagina dei dettagli degli standard, puoi anche abilitare i controlli in standard specifici. È necessario abilitare i controlli in standard specifici separatamente in ogni Account AWS e Regione AWS. Quando abiliti un controllo in standard specifici, ha effetto solo sull'account corrente e sulla regione.

Per abilitare un controllo in uno standard, devi prima abilitare almeno uno standard a cui si applica il controllo. Per istruzioni sull'attivazione di uno standard, vedereAbilitazione di uno standard di

sicurezza. Quando si abilita un controllo in uno o più standard, Security Hub CSPM inizia a generare i risultati per quel controllo. Security Hub CSPM include lo stato del controllo nel calcolo del punteggio di sicurezza complessivo e dei punteggi di sicurezza standard. Anche se abiliti un controllo in più standard, se attivi i risultati di controllo consolidati riceverai un unico risultato per ogni controllo di sicurezza tra gli standard. Per ulteriori informazioni, consulta Risultati dei controlli consolidati.

Per abilitare un controllo in uno standard, il controllo deve essere disponibile nella regione corrente. Per ulteriori informazioni, consulta Disponibilità dei controlli per regione.

Segui questi passaggi per abilitare un controllo CSPM di Security Hub in uno standard specifico. Al posto dei passaggi seguenti, puoi anche utilizzare l'azione `UpdateStandardsControl` API per abilitare i controlli in uno standard specifico. Per istruzioni su come abilitare un controllo in tutti gli standard, consultaCross-standard abilitazione in un unico account e regione.

Security Hub CSPM console

Per abilitare un controllo in uno standard specifico

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Scegli Standard di sicurezza dal pannello di navigazione.
3. Scegli Visualizza risultati per lo standard pertinente.
4. Seleziona un controllo.
5. Scegli Abilita controllo (questa opzione non viene visualizzata per un controllo già abilitato). Conferma scegliendo Abilita.

Security Hub CSPM API

Per abilitare un controllo in uno standard specifico

1. Esegui `ListSecurityControlDefinitions` e fornisci un ARN standard per ottenere un elenco dei controlli disponibili per uno standard specifico. Per ottenere un ARN standard, esegui. `DescribeStandards` Questa API restituisce ID di controllo di sicurezza indipendenti dallo standard, non ID di controllo specifici dello standard.

   Esempio di richiesta:

   ```
   {
   ```

```
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0"
}
```

2. Esegui `ListStandardsControlAssociations` e fornisci un ID di controllo specifico per restituire lo stato di abilitazione corrente di un controllo in ogni standard.

   Esempio di richiesta:

```
{
    "SecurityControlId": "IAM.1"
}
```

3. Esegui `BatchUpdateStandardsControlAssociations`. Fornisci l'ARN dello standard in cui desideri abilitare il controllo.
4. Imposta il `AssociationStatus` parametro uguale a. `ENABLED`

   Esempio di richiesta:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

Per abilitare un controllo in uno standard specifico

1. Esegui il `list-security-control-definitions` comando e fornisci un ARN standard per ottenere un elenco dei controlli disponibili per uno standard specifico. Per ottenere un ARN standard, esegui. `describe-standards` Questo comando restituisce ID di controllo di sicurezza indipendenti dallo standard, non ID di controllo specifici dello standard.

```
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. Esegui il `list-standards-control-associations` comando e fornisci un ID di controllo specifico per restituire lo stato di abilitazione corrente di un controllo in ogni standard.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Esegui il comando batch-update-standards-control-associations. Fornisci l'ARN dello standard in cui desideri abilitare il controllo.
4. Imposta il `AssociationStatus` parametro uguale a. `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"}]'
```

Abilitazione automatica di nuovi controlli negli standard abilitati

AWSSecurity Hub CSPM rilascia regolarmente nuovi controlli e li aggiunge a uno o più standard. Puoi scegliere se abilitare automaticamente i nuovi controlli negli standard abilitati.

Si consiglia di utilizzare la configurazione centrale CSPM di Security Hub per abilitare automaticamente nuovi controlli di sicurezza. È possibile creare policy di configurazione che includono un elenco di controlli da disabilitare in tutti gli standard. Tutti gli altri controlli, compresi quelli appena rilasciati, sono abilitati per impostazione predefinita. In alternativa, è possibile creare policy che includono un elenco di controlli da abilitare in tutti gli standard. Tutti gli altri controlli, compresi quelli appena rilasciati, sono disabilitati per impostazione predefinita. Per ulteriori informazioni, consulta Comprendere la configurazione centrale in Security Hub CSPM.

Security Hub CSPM non abilita nuovi controlli quando vengono aggiunti a uno standard che non hai abilitato.

Le seguenti istruzioni si applicano solo se non si utilizza la configurazione centrale.

Scegli il metodo di accesso preferito e segui i passaggi per abilitare automaticamente i nuovi controlli negli standard abilitati.

> **Note**
>
> Quando abiliti automaticamente i nuovi controlli utilizzando le seguenti istruzioni, puoi interagire con i controlli nella console e in modo programmatico subito dopo il rilascio.

Tuttavia, lo stato predefinito temporaneo dei controlli abilitati automaticamente è Disabilitato. Security Hub CSPM può impiegare fino a diversi giorni per elaborare la versione di controllo e designare il controllo come Attivato nel tuo account. Durante il periodo di elaborazione, è possibile abilitare o disabilitare manualmente un controllo e Security Hub CSPM manterrà tale designazione indipendentemente dal fatto che sia attivata l'abilitazione automatica del controllo.

Security Hub CSPM console

Per abilitare automaticamente i nuovi controlli

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli la scheda Generale.
3. In Controlli, scegli Modifica.
4. Attiva Auto-enable nuovi controlli negli standard abilitati.
5. Scegli Save (Salva).

Security Hub CSPM API

Per abilitare automaticamente nuovi controlli

1. Esegui `UpdateSecurityHubConfiguration`.
2. Per abilitare automaticamente nuovi controlli per gli standard abilitati, imposta `AutoEnableControls` su`true`. Se non desideri abilitare automaticamente i nuovi controlli, imposta `AutoEnableControls` su false.

AWS CLI

Per abilitare automaticamente i nuovi controlli

1. Esegui il comando `update-security-hub-configuration`.
2. Per abilitare automaticamente nuovi controlli per gli standard abilitati, specificare`--auto-enable-controls`. Se non desideri abilitare automaticamente i nuovi controlli, specifica`--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Comando di esempio

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Se non abiliti automaticamente i nuovi controlli, devi abilitarli manualmente. Per istruzioni, consulta Abilitazione dei controlli in Security Hub CSPM.

Disattivazione dei controlli in Security Hub CSPM

Per ridurre il rumore di ricerca, può essere utile disabilitare i controlli non pertinenti all'ambiente in uso. In AWS Security Hub CSPM, puoi disattivare un controllo per tutti gli standard di sicurezza o solo per standard specifici.

Se si disabilita un controllo per tutti gli standard, si verifica quanto segue:

- I controlli di sicurezza per il controllo non vengono più eseguiti.
- Non vengono generati ulteriori risultati per il controllo.
- I risultati esistenti non vengono più aggiornati per il controllo.
- I risultati esistenti per il controllo vengono archiviati automaticamente, in genere entro 3-5 giorni, nel migliore dei modi.
- Security Hub CSPM rimuove tutte le AWS Config regole correlate create per il controllo.

Se si disabilita un controllo solo per standard specifici, Security Hub CSPM interrompe l'esecuzione dei controlli di sicurezza per il controllo solo per tali standard. Ciò rimuove anche il controllo dai calcoli del punteggio di sicurezza per ciascuno di questi standard. Se il controllo è abilitato in altri standard, Security Hub CSPM mantiene la AWS Config regola associata, se applicabile, e continua a eseguire i controlli di sicurezza per il controllo degli altri standard. Security Hub CSPM include il controllo anche nel calcolo del punteggio di sicurezza per ciascuno degli altri standard, il che influisce sul punteggio di sicurezza riepilogativo.

Se disabiliti uno standard, tutti i controlli che si applicano allo standard vengono disattivati automaticamente per quello standard. Tuttavia, i controlli potrebbero continuare a essere abilitati in

altri standard. Quando si disabilita uno standard, Security Hub CSPM non tiene traccia dei controlli disattivati per lo standard. Di conseguenza, se successivamente si riattiva lo stesso standard, tutti i controlli ad esso applicabili vengono abilitati automaticamente. Per informazioni sulla disattivazione di uno standard, vedere. Disabilitazione di uno standard

La disattivazione di un controllo non è un'azione permanente. Supponiamo di disabilitare un controllo e quindi di abilitare uno standard che include il controllo. Il controllo viene quindi abilitato per tale standard. Quando si abilita uno standard in Security Hub CSPM, tutti i controlli che si applicano allo standard vengono abilitati automaticamente. Per informazioni sull'attivazione di uno standard, vedere. Abilitazione di uno standard

Argomenti

- Disattivazione di un controllo tra gli standard
- Disattivazione di un controllo in uno standard specifico
- Controlli consigliati da disabilitare in Security Hub CSPM

Disattivazione di un controllo tra gli standard

Ti consigliamo di disabilitare un controllo CSPM AWS di Security Hub tra gli standard per mantenere l'allineamento in tutta l'organizzazione. Se disabiliti un controllo solo in standard specifici, continuerai a ricevere i risultati del controllo se è abilitato in altri standard.

Cross-standard disattivazione in più account e regioni

Per disattivare un controllo di sicurezza su più Account AWS aree Regioni AWS, è necessario utilizzare la configurazione centrale.

Quando si utilizza la configurazione centrale, l'amministratore delegato può creare politiche di configurazione CSPM di Security Hub che disabilitano i controlli specifici tra gli standard abilitati. È quindi possibile associare la politica di configurazione a specifici account, unità organizzative o root. Una politica di configurazione ha effetto nella tua regione di origine (chiamata anche regione di aggregazione) e in tutte le regioni collegate.

Le politiche di configurazione offrono la personalizzazione. Ad esempio, puoi scegliere di disabilitare tutti i AWS CloudTrail controlli in un'unità organizzativa e puoi scegliere di disabilitare tutti i controlli IAM in un'altra unità organizzativa. Il livello di granularità dipende dagli obiettivi prefissati per la copertura della sicurezza nell'organizzazione. Per istruzioni sulla creazione di una politica di

configurazione che disabiliti i controlli specifici tra gli standard, consulta. Creazione e associazione di policy di configurazione

> **Note**
>
> L'amministratore delegato può creare politiche di configurazione per gestire i controlli in tutti gli standard tranne lo Service-Managed Standard:. AWS Control Tower I controlli per questo standard devono essere configurati nel AWS Control Tower servizio.

Se si desidera che alcuni account configurino i propri controlli anziché l'amministratore delegato, l'amministratore delegato può designare tali account come autogestiti. Self-managed gli account devono configurare i controlli separatamente in ciascuna regione.

Cross-standard disattivazione in un singolo account e regione

Se non utilizzi la configurazione centrale o sei un account autogestito, non puoi utilizzare i criteri di configurazione per disabilitare centralmente i controlli in più account e regioni. Tuttavia, puoi disabilitare un controllo in un singolo account e regione.

Security Hub CSPM console

Per disattivare un controllo tra gli standard in un account e in un'area geografica

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Scegli Controlli dal pannello di navigazione.
3. Scegli l'opzione accanto a un controllo.
4. Scegli Disabilita controllo. Questa opzione non viene visualizzata per un controllo già disabilitato.
5. Seleziona un motivo per disabilitare il controllo e conferma scegliendo Disabilita.
6. Ripeti l'operazione in ogni regione in cui desideri disattivare il controllo.

Security Hub CSPM API

Per disattivare un controllo tra gli standard in un account e in una regione

1. Richiama l'ListStandardsControlAssociationsAPI. Fornisci un ID di controllo di sicurezza.

Esempio di richiesta:

```
{
    "SecurityControlId": "IAM.1"
}
```

2. Richiama l'BatchUpdateStandardsControlAssociationsAPI. Fornisci l'ARN di tutti gli standard in cui è abilitato il controllo. Per ottenere ARN standard, esegui. `DescribeStandards`
3. Imposta il `AssociationStatus` parametro uguale a. `DISABLED` Se segui questi passaggi per un controllo già disabilitato, l'API restituisce una risposta con codice di stato HTTP 200.

   Esempio di richiesta:

```
{
    "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. Ripetere l'operazione in ogni regione in cui si desidera disattivare il controllo.

AWS CLI

Per disattivare un controllo tra gli standard in un account e in una regione

1. Esegui il comando list-standards-control-associations. Fornisci un ID per il controllo di sicurezza.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Esegui il comando batch-update-standards-control-associations. Fornisci l'ARN di tutti gli standard in cui è abilitato il controllo. Per ottenere ARN standard, esegui il `describe-standards` comando.

3. Imposta il `AssociationStatus` parametro uguale a. `DISABLED` Se segui questi passaggi per un controllo già disabilitato, il comando restituisce una risposta con codice di stato HTTP 200.

```
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. Ripeti l'operazione in ogni regione in cui desideri disattivare il controllo.

Disattivazione di un controllo in uno standard specifico

È possibile disattivare un controllo solo in specifici standard di sicurezza, anziché in tutti gli standard. Se il controllo si applica ad altri standard abilitati, AWS Security Hub CSPM continua a eseguire i controlli di sicurezza relativi al controllo e l'utente continua a ricevere i risultati del controllo.

Si consiglia di allineare lo stato di abilitazione di un controllo tra tutti gli standard abilitati a cui si applica il controllo. Per informazioni sulla disattivazione di un controllo in tutti gli standard a cui si applica, vedere. Disattivazione di un controllo tra gli standard

Nella pagina dei dettagli degli standard, puoi anche disattivare i controlli in standard specifici. È necessario disabilitare i controlli in standard specifici separatamente in ciascuno Account AWS e Regione AWS. La disattivazione di un controllo in standard specifici ha effetto solo sull'account corrente e sulla regione.

Scegli il tuo metodo preferito e segui questi passaggi per disabilitare un controllo in uno o più standard specifici.

Security Hub CSPM console

Per disattivare un controllo in uno standard specifico

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

2. Scegli Standard di sicurezza dal pannello di navigazione. Scegli Visualizza risultati per lo standard pertinente.
3. Seleziona un controllo.
4. Scegli Disabilita controllo. Questa opzione non viene visualizzata per un controllo già disabilitato.
5. Fornisci un motivo per disabilitare il controllo e conferma scegliendo Disabilita.

Security Hub CSPM API

Per disattivare un controllo in uno standard specifico

1. Esegui `ListSecurityControlDefinitions` e fornisci un ARN standard per ottenere un elenco dei controlli disponibili per uno standard specifico. Per ottenere un ARN standard, esegui. `DescribeStandards` Questa API restituisce ID di controllo di sicurezza indipendenti dallo standard, non ID di controllo specifici dello standard.

   Esempio di richiesta:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Esegui `ListStandardsControlAssociations` e fornisci un ID di controllo specifico per restituire lo stato di abilitazione corrente di un controllo in ogni standard.

   Esempio di richiesta:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Esegui `BatchUpdateStandardsControlAssociations`. Fornisci l'ARN dello standard in cui desideri disabilitare il controllo.
4. Imposta il `AssociationStatus` parametro uguale a. `DISABLED` Se segui questi passaggi per un controllo già disabilitato, l'API restituisce una risposta con codice di stato HTTP 200.

   Esempio di richiesta:

```
{
    "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

Per disattivare un controllo in uno standard specifico

1. Esegui il `list-security-control-definitions` comando e fornisci un ARN standard per ottenere un elenco dei controlli disponibili per uno standard specifico. Per ottenere un ARN standard, esegui. `describe-standards` Questo comando restituisce ID di controllo di sicurezza indipendenti dallo standard, non ID di controllo specifici dello standard.

```
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. Esegui il `list-standards-control-associations` comando e fornisci un ID di controllo specifico per restituire lo stato di abilitazione corrente di un controllo in ogni standard.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Esegui il comando `batch-update-standards-control-associations`. Fornisci l'ARN dello standard in cui desideri disabilitare il controllo.
4. Imposta il `AssociationStatus` parametro uguale a. `DISABLED` Se segui questi passaggi per un controllo già abilitato, il comando restituisce una risposta con codice di stato HTTP 200.

```
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"}]'
```

Controlli consigliati da disabilitare in Security Hub CSPM

Ti consigliamo di disabilitare alcuni controlli CSPM AWS di Security Hub per ridurre il rumore di ricerca e i costi di utilizzo.

Controlli che utilizzano risorse globali

Alcuni Servizi AWS supportano risorse globali, il che significa che puoi accedere alla risorsa da qualsiasiRegione AWS. Per risparmiare sui costi diAWS Config, puoi disabilitare la registrazione delle risorse globali in tutte le regioni tranne una. Dopo aver eseguito questa operazione, tuttavia, Security Hub CSPM continua a eseguire i controlli di sicurezza in tutte le regioni in cui è abilitato un controllo e ti addebita in base al numero di controlli per account per regione. Di conseguenza, per ridurre i rumori di ricerca e risparmiare sui costi di Security Hub CSPM, è necessario disabilitare anche i controlli che coinvolgono risorse globali in tutte le regioni ad eccezione della regione che registra le risorse globali.

Se un controllo coinvolge risorse globali ma è disponibile in una sola regione, disabilitarlo in quella regione impedisce di ottenere risultati sulla risorsa sottostante. In questo caso, consigliamo di mantenere il controllo abilitato. Quando si utilizza l'aggregazione tra regioni, la regione in cui è disponibile il controllo deve essere la regione di aggregazione o una delle regioni collegate. I seguenti controlli coinvolgono risorse globali ma sono disponibili solo in una singola regione:

- Tutti i CloudFront controlli: disponibili solo nella regione Stati Uniti orientali (Virginia settentrionale)
- GlobalAccelerator.1— Disponibile solo nella regione Stati Uniti occidentali (Oregon)
- Route53.2— Disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)
- WAF.1, WAF.6, WAF.7, WAF.8 — Disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

> **Note**
>
> Se si utilizza la configurazione centrale, Security Hub CSPM disattiva automaticamente i controlli che coinvolgono risorse globali in tutte le regioni tranne la regione di origine. Gli altri controlli che scegli di abilitare tramite una politica di configurazione sono abilitati in tutte le regioni in cui sono disponibili. Per limitare i risultati di questi controlli a una sola regione, puoi aggiornare le impostazioni del AWS Config registratore e disattivare la registrazione globale delle risorse in tutte le regioni tranne la regione d'origine.
> Se un controllo abilitato che coinvolge risorse globali non è supportato nella regione di origine, Security Hub CSPM tenta di abilitare il controllo in una regione collegata in cui il

controllo è supportato. Con la configurazione centralizzata, ti manca la copertura per un controllo che non è disponibile nella regione d'origine o in nessuna delle regioni collegate. Per ulteriori informazioni sulla configurazione centralizzata, consultaComprendere la configurazione centrale in Security Hub CSPM.

Per i controlli che hanno un tipo di pianificazione periodica, è necessario disabilitarli in Security Hub CSPM per impedire la fatturazione. L'impostazione del AWS Config parametro `includeGlobalResourceTypes` su `false` non influisce sui controlli periodici CSPM di Security Hub.

I seguenti controlli CSPM di Security Hub utilizzano risorse globali:

- [Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate

- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
- [IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
- [IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
- [IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
- [IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
- [IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
- [IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS

- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

CloudTrail controlli di registrazione

Il CloudTrail.2controllo valuta l'uso di AWS Key Management Service (AWS KMS) per AWS CloudTrail crittografare i log delle tracce. Se si registrano questi percorsi in un account di registrazione centralizzato, è necessario abilitare questo controllo solo nell'account e Regione AWS dove avviene la registrazione centralizzata.

Se si utilizza la configurazione centrale, lo stato di attivazione di un controllo è allineato tra la regione di origine e le regioni collegate. Non è possibile disabilitare un controllo in alcune regioni e abilitarlo in altre. In questo caso, puoi eliminare i risultati dal CloudTrail.2 controllo per ridurre i disturbi rilevati.

CloudWatch controlli di allarme

Se preferisci utilizzare Amazon GuardDuty per il rilevamento delle anomalie anziché gli CloudWatch allarmi Amazon, puoi disabilitare i seguenti controlli, che si concentrano sugli CloudWatch allarmi:

- [CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»
- [CloudWatch.2] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate
- [CloudWatch.3] Assicurati che esistano un filtro metrico di registro e un allarme per l'accesso alla console di gestione senza MFA
- [CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM
- [CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrail alla configurazione
- [CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per Console di gestione AWS errori di autenticazione

- [CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione pianificata delle chiavi gestite dal cliente
- [CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3
- [CloudWatch.9] Assicurati che esistano un filtro metrico di registro e un allarme per AWS Config modifiche alla configurazione
- [CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza
- [CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)
- [CloudWatch.12] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gateway di rete
- [CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte
- [CloudWatch.14] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche al VPC

Comprensione dei controlli e dei punteggi di sicurezza in Security Hub CSPM

Per ogni controllo abilitato, AWS Security Hub CSPM esegue controlli di sicurezza. Un controllo di sicurezza produce un risultato che indica se una AWS risorsa specifica è conforme alle regole incluse nel controllo.

Alcuni controlli vengono eseguiti secondo una pianificazione periodica. Altri controlli vengono eseguiti solo quando si modifica lo stato della risorsa. Per ulteriori informazioni, consulta Pianificazione dell'esecuzione dei controlli di sicurezza.

Molti controlli di sicurezza utilizzano regole AWS Config gestite o personalizzate per stabilire i requisiti di conformità. Per eseguire questi controlli, è necessario configurare AWS Config e attivare la registrazione delle risorse per le risorse necessarie. Per ulteriori informazioni sulla configurazioneAWS Config, vedereAttivazione e configurazione AWS Config per Security Hub CSPM. Per un elenco delle AWS Config risorse che è necessario registrare per ogni standard, vedereRichiesto AWS Config risorse per i risultati del controllo. Altri controlli utilizzano funzioni Lambda personalizzate, gestite da Security Hub CSPM e non richiedono alcun prerequisito.

Poiché Security Hub CSPM esegue i controlli di sicurezza, genera i risultati e assegna loro uno stato di conformità. Per ulteriori informazioni sullo stato di conformità, vedere. Valutazione dello stato di conformità dei risultati del Security Hub CSPM

Security Hub CSPM utilizza lo stato di conformità dei risultati del controllo per determinare lo stato di controllo generale. In base allo stato del controllo, Security Hub CSPM calcola anche un punteggio di sicurezza per tutti i controlli abilitati e per standard specifici. Per ulteriori informazioni, consultare the section called "Stato di conformità e stato di controllo" e the section called "Calcolo dei punteggi di sicurezza".

Se hai attivato i risultati del controllo consolidato, Security Hub CSPM genera un singolo risultato anche quando un controllo è associato a più di uno standard. Per ulteriori informazioni, consulta Risultati di controllo consolidati.

Argomenti

- Richiesto AWS Config risorse per i risultati del controllo
- Pianificazione dell'esecuzione dei controlli di sicurezza
- Generazione e aggiornamento dei risultati di controllo
- Valutazione dello stato di conformità e dello stato di controllo
- Calcolo dei punteggi di sicurezza

Richiesto AWS Config risorse per i risultati del controllo

> **Note**
>
> Se utilizzi Security Hub CSPM e Security Hub, la configurazione della registrazione delle risorse viene gestita automaticamente. Security Hub crea un registratore di configurazione collegato al servizio con AWS Config e ottiene informazioni dirette su tutte le risorse correlate ai controlli supportati in Security Hub CSPM. Per ulteriori informazioni, consulta Utilizzo del registratore di configurazione collegato al servizio.

In AWS Security Hub CSPM, alcuni controlli utilizzano AWS Config regole collegate ai servizi che rilevano le modifiche alla configurazione nelle risorse. AWS Affinché Security Hub CSPM generi risultati accurati per questi controlli, è necessario abilitare AWS Config e attivare la registrazione delle risorse. AWS Config Per informazioni su come Security Hub CSPM utilizza AWS Config le regole e su come abilitarle e configurarle AWS Config, vedere. Attivazione e configurazione AWS Config per

Security Hub CSPM Per informazioni dettagliate sulla registrazione delle risorse, consulta Lavorare con il registratore di configurazione nella Guida per gli AWS Config sviluppatori.

Per ricevere risultati di controllo accurati, è necessario attivare la registrazione AWS Config delle risorse per i controlli abilitati con un tipo di pianificazione innescato dalla modifica. Alcuni controlli con un tipo di pianificazione periodica richiedono anche la registrazione delle risorse. Questa pagina elenca le risorse necessarie per questi controlli CSPM di Security Hub.

I controlli CSPM di Security Hub possono basarsi su AWS Config regole gestite o regole CSPM Security Hub personalizzate. Assicurati che non esistano policy AWS Identity and Access Management (IAM) o policy AWS Organizations gestite che AWS Config impediscano di avere l'autorizzazione a registrare le tue risorse. I controlli CSPM di Security Hub valutano direttamente le configurazioni delle risorse e non tengono conto delle AWS Organizations politiche.

> **Note**
>
> Regioni AWS Se un controllo non è disponibile, la risorsa corrispondente non è disponibile in. AWS Config Per un elenco di questi limiti, consultaLimiti regionali sui controlli CSPM di Security Hub.

Argomenti

- Risorse necessarie per tutti i controlli CSPM di Security Hub
- Risorse necessarie per AWS Standard di best practice di sicurezza di base
- Risorse necessarie per il CIS AWS Foundations Benchmark
- Risorse necessarie per lo standard NIST SP 800-53 Revisione 5
- Risorse necessarie per lo standard NIST SP 800-171 Revision 2
- Risorse richieste per PCI DSS v3.2.1
- Risorse necessarie per AWS Standard di etichettatura delle risorse

Risorse necessarie per tutti i controlli CSPM di Security Hub

Affinché Security Hub CSPM generi risultati per i controlli attivati dalle modifiche che sono abilitati e utilizzano una AWS Config regola, è necessario registrare i seguenti tipi di risorse in. AWS Config Questa tabella indica anche quali controlli valutano un particolare tipo di risorsa. Un singolo controllo può valutare più di un tipo di risorsa.

Servizio AWS	Tipi di risorse	Controlli correlati
AWS Amplify	`AWS::Amplify::App`	Amplify.1
	`AWS::Amplify::Branch`	Amplify.2
Gateway Amazon API	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3 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

Servizio AWS	Tipi di risorse	Controlli correlati
	`AWS::AppConfig::ExtensionAssociation`	AppConfig.4
Amazon AppFlow	`AWS::AppFlow::Flow`	AppFlow.1
AWS App Runner	`AWS::AppRunner::Service`	AppRunner.1
	`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

Servizio AWS	Tipi di risorse	Controlli correlati
AWS Batch	`AWS::Batch::ComputeEnvironment`	Batch.3 Batch.4
	`AWS::Batch::JobQueue`	Batch.1
	`AWS::Batch::SchedulingPolicy`	Batch.2
Amazon Bedrock	`AWS::Bedrock::DataSource`	Bedrock.1
Amazon Bedrock 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

Servizio AWS	Tipi di risorse	Controlli correlati
	`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::Athena::WorkGroup`	Athena.3 Athena.4
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.2 CloudFormation.3 CloudFormation.4

Servizio AWS	Tipi di risorse	Controlli correlati
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::CloudTrail::EventDataStore`	CloudTrail.11
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17

Servizio AWS	Tipi di risorse	Controlli correlati
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
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	CodeGuruProfiler.1
CodeGuru Revisore Amazon	`AWS::CodeGuruReviewer::RepositoryAssociation`	CodeGuruReviewer.1
Amazon Cognito	`AWS::Cognito::IdentityPool`	Cognito.2

Servizio AWS	Tipi di risorse	Controlli correlati
	`AWS::Cognito::UserPool`	Cognito.1 Cognito.3 Cognito.4 Cognito.5 Cognito.6
Cliente Amazon Connect	`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::DMS::EventSubscription`	DMS.3

Servizio AWS	Tipi di risorse	Controlli correlati
	`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::EC2::EIP`	EC2.12 EC2.37

Servizio AWS	Tipi di risorse	Controlli correlati
	`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::EC2::NetworkAcl`	EC2.16 EC2.21 EC2.41

Servizio AWS	Tipi di risorse	Controlli correlati
	`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::EC2::Subnet`	EC2.15 EC2.44 ElastiCache.7

Servizio AWS	Tipi di risorse	Controlli correlati
	`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::EC2::VPC`	EC2.6 EC2.46

Servizio AWS	Tipi di risorse	Controlli correlati
	`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::AutoScaling::LaunchConfiguration`	AutoScaling.3 Autoscaling.5

Servizio AWS	Tipi di risorse	Controlli correlati
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::ECS::Service`	ECS.2 ECS.10 ECS.13

Servizio AWS	Tipi di risorse	Controlli correlati
	`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
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`	EKS.2 EKS.6 EKS.8

Servizio AWS	Tipi di risorse	Controlli correlati
	`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

Servizio AWS	Tipi di risorse	Controlli correlati
	`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

Servizio AWS	Tipi di risorse	Controlli correlati
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

Servizio AWS	Tipi di risorse	Controlli correlati
AWS Identity and Access Management (IAM)	`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

Servizio AWS	Tipi di risorse	Controlli correlati
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

Servizio AWS	Tipi di risorse	Controlli correlati
	`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

Servizio AWS	Tipi di risorse	Controlli correlati
	`AWS::IoTWireless::ServiceProfile`	IoTWireless.2
	`AWS::IoTWireless::FuotaTask`	IoTWireless.3
Amazon Keyspaces (per 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

Servizio AWS	Tipi di risorse	Controlli correlati
MSK Amazon	`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

Servizio AWS	Tipi di risorse	Controlli correlati
OpenSearch Servizio Amazon	`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

Servizio AWS	Tipi di risorse	Controlli correlati
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

Servizio AWS	Tipi di risorse	Controlli correlati
		RDS.37 RDS.47 RDS.48
	`AWS::RDS::DBClusterSnapshot`	DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29

Servizio AWS	Tipi di risorse	Controlli correlati
	`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

Servizio AWS	Tipi di risorse	Controlli correlati
	`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

Servizio AWS	Tipi di risorse	Controlli correlati
	`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

Servizio AWS	Tipi di risorse	Controlli correlati
	`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

Servizio AWS	Tipi di risorse	Controlli correlati
	`AWS::S3Express::DirectoryBucket`	S3.25
Amazon SageMaker AI	`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

Servizio AWS	Tipi di risorse	Controlli correlati
	`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
Servizio di notifica semplice Amazon (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

Servizio AWS	Tipi di risorse	Controlli correlati
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

Servizio AWS	Tipi di risorse	Controlli correlati
	`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

Risorse necessarie per AWS Standard di best practice di sicurezza di base

Affinché Security Hub CSPM riporti in modo accurato i risultati relativi ai controlli attivati dalle modifiche che si applicano allo standard AWS Foundational Security Best Practices (v.1.0.0), sono abilitati e utilizzano una AWS Config regola, è necessario registrare i seguenti tipi di risorse in. AWS Config Per informazioni su questo standard, vedere. AWS Standard di best practice di sicurezza di base in Security Hub CSPM

Servizio AWS	Tipi di risorse
Gateway Amazon API	`AWS::ApiGateway::DomainName` , `AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`

Servizio AWS	Tipi di risorse
AWS AppSync	`AWS::AppSync::ApiCache` , `AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Bedrock	`AWS::Bedrock::DataSource`
Amazon Bedrock 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`
Cliente Amazon Connect	`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`

Servizio AWS	Tipi di risorse
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`

Servizio AWS	Tipi di risorse
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 Servizio Amazon	`AWS::OpenSearch::Domain`

Servizio AWS	Tipi di risorse
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 AI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::InferenceExperiment` , `AWS::SageMaker::Model` , `AWS::SageMaker::ModelExplainabilityJobDefinition` , `AWS::SageMaker::ModelQualityJobDefinition` , `AWS::SageMaker::MonitoringSchedule` , `AWS::SageMaker::NotebookInstance`
Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Servizio AWS	Tipi di risorse
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`

Risorse necessarie per il CIS AWS Foundations Benchmark

Per eseguire controlli di sicurezza per i controlli abilitati che si applicano al benchmark Center for Internet Security (CIS) AWS Foundations, Security Hub CSPM esegue le esatte fasi di controllo prescritte per i controlli o utilizza regole gestite specifiche. AWS Config Per informazioni su questo standard in Security Hub CSPM, vedere. CIS AWS Benchmark dei fondamenti nel Security Hub CSPM

Risorse necessarie per CIS v5.0.0

Affinché Security Hub CSPM riporti in modo accurato i risultati dei controlli attivati da modifiche CIS v5.0.0 abilitati che utilizzano una AWS Config regola, è necessario registrare i seguenti tipi di risorse in. AWS Config

Servizio AWS	Tipi di risorse
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`

Servizio AWS	Tipi di risorse
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`

Risorse necessarie per CIS v3.0.0

Affinché Security Hub CSPM riporti in modo accurato i risultati dei controlli attivati da modifiche CIS v3.0.0 abilitati che utilizzano una AWS Config regola, è necessario registrare i seguenti tipi di risorse in. AWS Config

Servizio AWS	Tipi di risorse
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`

Risorse necessarie per CIS v1.4.0

Affinché Security Hub CSPM riporti in modo accurato i risultati dei controlli attivati da modifiche CIS v1.4.0 abilitati che utilizzano una AWS Config regola, è necessario registrare i seguenti tipi di risorse in. AWS Config

Servizio AWS	Tipi di risorse
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`

Risorse richieste per CIS v1.2.0

Affinché Security Hub CSPM riporti in modo accurato i risultati dei controlli attivati da modifiche CIS v1.2.0 abilitati che utilizzano una AWS Config regola, è necessario registrare i seguenti tipi di risorse in. AWS Config

Servizio AWS	Tipi di risorse
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`

Risorse necessarie per lo standard NIST SP 800-53 Revisione 5

Affinché Security Hub CSPM riporti con precisione i risultati relativi ai controlli attivati dalle modifiche che si applicano allo standard NIST SP 800-53 Revisione 5, sono abilitati e utilizzano una AWS Config regola, è necessario registrare i seguenti tipi di risorse in. AWS Config Per informazioni su questo standard, vedere. NIST SP 800-53 Revisione 5 nel Security Hub CSPM

Servizio AWS	Tipi di risorse
Gateway Amazon API	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`

Servizio AWS	Tipi di risorse
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Bedrock 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`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Servizio AWS	Tipi di risorse
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 (IAM)	`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`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`

Servizio AWS	Tipi di risorse
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
OpenSearch Servizio Amazon	`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`
Servizio di notifica semplice Amazon (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`
Amazon SageMaker AI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::NotebookInstance`

Servizio AWS	Tipi di risorse
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`

Risorse necessarie per lo standard NIST SP 800-171 Revision 2

Affinché Security Hub CSPM riporti in modo accurato i risultati relativi ai controlli attivati dalle modifiche che si applicano allo standard NIST SP 800-171 Revisione 2, sono abilitati e utilizzano una AWS Config regola, è necessario registrare i seguenti tipi di risorse in. AWS Config Per informazioni su questo standard, vedere. NIST SP 800-171 Revisione 2 nel Security Hub CSPM

Servizio AWS	Tipi di risorse
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
Gateway Amazon API	`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`

Servizio AWS	Tipi di risorse
AWS Identity and Access Management(IAM)	`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`
Servizio Amazon Simple Storage (Amazon S3)	`AWS::S3::Bucket`
Servizio di notifica semplice di Amazon (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SSM)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

Risorse richieste per PCI DSS v3.2.1

Affinché Security Hub CSPM riporti in modo accurato i risultati dei controlli che si applicano alla versione 3.2.1 del Payment Card Industry Data Security Standard (PCI DSS), sono abilitati e utilizzano una AWS Config regola, è necessario registrare i seguenti tipi di risorse in. AWS Config Per informazioni su questo standard, vedere. PCI DSS nel Security Hub CSPM

Servizio AWS	Tipi di risorse
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 Identity and Access Management (IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Lambda	`AWS::Lambda::Function`

Servizio AWS	Tipi di risorse
OpenSearch Servizio Amazon	`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`

Risorse necessarie per AWS Standard di etichettatura delle risorse

Tutti i controlli che si applicano allo standard AWS Resource Tagging attivano una modifica e utilizzano una regola. AWS Config Affinché Security Hub CSPM riporti in modo accurato i risultati di questi controlli, è necessario registrare i seguenti tipi di risorse in. AWS Config Per informazioni su questo standard, vedere. AWS Standard di etichettatura delle risorse in Security Hub CSPM

Servizio AWS	Tipi di risorse
AWS Amplify	`AWS::Amplify::App` , `AWS::Amplify::Branch`
Amazon AppFlow	`AWS::AppFlow::Flow`
AWS App Runner	`AWS::AppRunner::Service` , `AWS::AppRunner::VpcConnector`
AWS AppConfig	`AWS::AppConfig::Application` , `AWS::AppConfig::ConfigurationProfile` , `AWS::AppConfig::En`

Servizio AWS	Tipi di risorse
	`vironment` , `AWS::AppConfig::Extensi onAssociation`
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`
Cliente Amazon Connect	`AWS::CustomerProfiles::ObjectType`

Servizio AWS	Tipi di risorse

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`
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`

Servizio AWS	Tipi di risorse
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`
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 (IAM)	`AWS::IAM::Role` , `AWS::IAM::User`

Servizio AWS	Tipi di risorse
AWS Identity and Access Management Access Analyzer (Analizzatore di accesso IAM)	`AWS::AccessAnalyzer::Analyzer`
AWS IoT	`AWS::IoT::Authorizer` , `AWS::IoT::Dimension` , `AWS::IoT::MitigationAction` , `AWS::IoT::Policy` , `AWS::IoT::RoleAlias` , `AWS::IoT::SecurityProfile`
AWS IoT Eventi	`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 Wireless	`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 (per Apache Cassandra)	`AWS::Cassandra::Keyspace`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`

Servizio AWS	Tipi di risorse
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy`
OpenSearch Servizio Amazon	`AWS::OpenSearch::Domain`
AWS Autorità di certificazione privata	`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 AI	`AWS::SageMaker::AppImageConfig` , `AWS::SageMaker::Image`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet` , `AWS::SES::ContactList`
Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))	`AWS::SNS::Topic`

Servizio AWS	Tipi di risorse
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Systems Manager (SSM)	`AWS::SSM::Document`
AWS Transfer Family	`AWS::Transfer::Agreement` , `AWS::Transfer::Certificate` , `AWS::Transfer::Connector` , `AWS::Transfer::Profile` , `AWS::Transfer::Workflow`

Pianificazione dell'esecuzione dei controlli di sicurezza

Dopo aver abilitato uno standard di sicurezza, AWS Security Hub CSPM inizia a eseguire tutti i controlli entro due ore. La maggior parte dei controlli inizia entro 25 minuti. Security Hub CSPM esegue i controlli valutando la regola alla base di un controllo. Fino a quando un controllo non completa la prima esecuzione dei controlli, lo stato è Nessun dato.

Quando abiliti un nuovo standard, potrebbero essere necessarie fino a 24 ore prima che Security Hub CSPM generi risultati per i controlli che utilizzano la stessa regola sottostante AWS Config collegata ai servizi dei controlli abilitati di altri standard abilitati. Ad esempio, se abiliti il Lambda.1controllo nello standard AWS Foundational Security Best Practices (FSBP), Security Hub CSPM crea la regola collegata al servizio e in genere genera i risultati in pochi minuti. Dopodiché, se abiliti il Lambda.1 controllo nel Payment Card Industry Data Security Standard (PCI DSS), potrebbero essere necessarie fino a 24 ore prima che Security Hub CSPM generi i risultati per il controllo, poiché utilizza la stessa regola collegata al servizio.

Dopo il controllo iniziale, la pianificazione di ogni controllo può essere periodica o attivata a modifiche. Per un controllo basato su una AWS Config regola gestita, la descrizione del controllo include un collegamento alla descrizione della regola nella Guida per gli AWS Configsviluppatori. Tale descrizione specifica se la regola è soggetta a modifiche o è periodica.

Controlli di sicurezza periodici

I controlli di sicurezza periodici vengono eseguiti automaticamente entro 12 o 24 ore dall'esecuzione più recente. Security Hub CSPM determina la periodicità e non è possibile modificarla. I controlli periodici riflettono una valutazione nel momento in cui viene eseguito il controllo.

Se si aggiorna lo stato del flusso di lavoro di un risultato di controllo periodico e quindi nel controllo successivo lo stato di conformità del risultato rimane lo stesso, lo stato del flusso di lavoro rimane modificato. Ad esempio, se non riesci a trovare il KMS.4controllo (la AWS KMS keyrotazione deve essere abilitata) e quindi correggi il risultato, Security Hub CSPM modifica lo stato del flusso di lavoro da a. `NEW` `RESOLVED` Se si disabilita la rotazione delle chiavi KMS prima del successivo controllo periodico, lo stato del flusso di lavoro del risultato rimane invariato. `RESOLVED`

I controlli che utilizzano le funzioni Lambda personalizzate di Security Hub CSPM sono periodici.

Change-triggered controlli di sicurezza

Change-triggered i controlli di sicurezza vengono eseguiti quando la risorsa associata cambia stato. AWS Configconsente di scegliere tra la registrazione continua delle modifiche dello stato delle risorse e la registrazione giornaliera. Se si sceglie la registrazione giornaliera, AWS Config fornisce i dati di configurazione delle risorse alla fine di ogni periodo di 24 ore in caso di cambiamenti nello stato delle risorse. Se non ci sono modifiche, non viene fornito alcun dato. Ciò può ritardare la generazione dei risultati CSPM di Security Hub fino al completamento di un periodo di 24 ore. Indipendentemente dal periodo di registrazione scelto, Security Hub CSPM verifica almeno una volta ogni 24 ore per assicurarsi che nessun aggiornamento delle risorse sia AWS Config stato perso.

In generale, Security Hub CSPM utilizza regole attivate dalle modifiche quando possibile. Affinché una risorsa utilizzi una regola attivata da una modifica, deve supportare gli elementi di configurazione. AWS Config

Generazione e aggiornamento dei risultati di controllo

AWSSecurity Hub CSPM genera e aggiorna i risultati dei controlli quando esegue controlli di sicurezza. I risultati del controllo utilizzano il AWSSecurity Finding Format (ASFF).

Security Hub CSPM normalmente addebita un costo per ogni controllo di sicurezza. Tuttavia, se più controlli utilizzano la stessa AWS Config regola, Security Hub CSPM addebita solo una volta per ogni controllo rispetto alla regola. Ad esempio, la AWS Config `iam-password-policy` regola viene utilizzata da più controlli nello standard CIS AWS Foundations Benchmark e nello standard AWS

Foundational Security Best Practices. Ogni volta che Security Hub CSPM esegue un controllo rispetto a tale regola, genera un risultato di controllo separato per ogni controllo correlato, ma addebita una sola volta per il controllo.

Se la dimensione di un risultato di controllo supera il massimo di 240 KB, Security Hub CSPM rimuove l'`Resource.Details`oggetto dal risultato. Per i controlli supportati da AWS Config risorse, è possibile rivedere i dettagli delle risorse utilizzando la console. AWS Config

Argomenti

- Risultati di controllo consolidati
- Generazione, aggiornamento e archiviazione dei risultati di controllo
- Automazione e soppressione dei risultati del controllo
- Dettagli sulla conformità per i risultati del controllo
- ProductFields dettagli relativi ai risultati del controllo
- Livelli di gravità per i risultati del controllo

Risultati di controllo consolidati

Se i risultati del controllo consolidato sono abilitati per il tuo account, Security Hub CSPM genera un singolo risultato o aggiornamento dei risultati per ogni controllo di sicurezza di un controllo, anche se un controllo si applica a più standard abilitati. Per un elenco dei controlli e degli standard a cui si applicano, consulta la. Riferimento di controllo per Security Hub CSPM Si consiglia di abilitare risultati di controllo consolidati per ridurre il rumore di rilevamento.

Se hai abilitato Security Hub CSPM Account AWS prima del 23 febbraio 2023, puoi abilitare i risultati del controllo consolidato seguendo le istruzioni riportate più avanti in questa sezione. Se abiliti Security Hub CSPM a partire dal 23 febbraio 2023, i risultati del controllo consolidato vengono abilitati automaticamente per il tuo account.

Se utilizzi l'integrazione CSPM di Security Hub con AWS Organizations o account membro invitati tramite una procedura di invito manuale, i risultati del controllo consolidato sono abilitati per gli account membro solo se sono abilitati per l'account amministratore. Se la funzionalità è disabilitata per l'account amministratore, è disabilitata per gli account dei membri. Questo comportamento si applica agli account membro nuovi ed esistenti. Inoltre, se l'amministratore utilizza la configurazione centrale per gestire Security Hub CSPM per più account, non può utilizzare policy di configurazione centrale per abilitare o disabilitare i risultati del controllo consolidato per gli account.

Se disabiliti i risultati del controllo consolidato per il tuo account, Security Hub CSPM genera o aggiorna un risultato di controllo separato per ogni standard abilitato che include un controllo. Ad esempio, se abiliti quattro standard che condividono un controllo, ricevi quattro risultati separati dopo un controllo di sicurezza per il controllo. Se abiliti i risultati del controllo consolidato, riceverai solo un risultato.

Quando abiliti i risultati del controllo consolidato, Security Hub CSPM crea nuovi risultati indipendenti dallo standard e archivia i risultati originali basati sullo standard. Alcuni campi e valori di controllo relativi alla ricerca cambieranno, il che potrebbe influire sui flussi di lavoro esistenti. Per informazioni su queste modifiche, consultaRisultati di controllo consolidati: modifiche ASFF. L'abilitazione dei risultati del controllo consolidato potrebbe influire anche sui risultati che i prodotti integrati di terze parti ricevono da Security Hub CSPM. Se utilizzi la soluzione Automated Security Response on AWS v2.0.0, tieni presente che supporta i risultati del controllo consolidato.

Per abilitare o disabilitare i risultati del controllo consolidato, è necessario accedere a un account amministratore o a un account autonomo.

> **Note**
>
> Dopo aver abilitato i risultati del controllo consolidato, possono essere necessarie fino a 24 ore prima che Security Hub CSPM generi nuovi risultati consolidati e archivi i risultati esistenti basati sugli standard. Allo stesso modo, dopo aver disabilitato i risultati del controllo consolidato, possono essere necessarie fino a 24 ore prima che Security Hub CSPM generi nuovi risultati basati su standard e archivi i risultati consolidati esistenti. In questi periodi, potresti visualizzare nel tuo account un mix di risultati indipendenti dagli standard e basati sugli standard.

Security Hub CSPM console

Per abilitare o disabilitare i risultati del controllo consolidato

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, in Settings (Impostazioni), scegliere General (Generali).
3. Nella sezione Controlli, scegli Modifica.
4. Utilizzate l'interruttore Consolidated control results (Risultati di controllo consolidati) per abilitare o disabilitare i risultati del controllo consolidato.

5. Scegli Save (Salva).

Security Hub CSPM API

Per abilitare o disabilitare i risultati del controllo consolidato a livello di codice, utilizzate il UpdateSecurityHubConfigurationfunzionamento dell'API CSPM Security Hub. Oppure, se utilizzi il, esegui il AWS CLI comando. update-security-hub-configuration

Per il `control-finding-generator` parametro, specificate `SECURITY_CONTROL` se abilitare i risultati del controllo consolidato. Per disabilitare i risultati del controllo consolidato, specificare. `STANDARD_CONTROL`

Ad esempio, il AWS CLI comando seguente abilita i risultati di controllo consolidati.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

Il AWS CLI comando seguente disabilita i risultati del controllo consolidato.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Generazione, aggiornamento e archiviazione dei risultati di controllo

Security Hub CSPM esegue i controlli di sicurezza in base a una pianificazione. La prima volta che Security Hub CSPM esegue un controllo di sicurezza, genera un nuovo risultato per ogni AWS risorsa controllata dal controllo. Ogni volta che Security Hub CSPM esegue successivamente un controllo di sicurezza per il controllo, aggiorna i risultati esistenti per riportare i risultati del controllo. Ciò significa che è possibile utilizzare i dati forniti dai singoli risultati per tenere traccia delle modifiche di conformità per particolari risorse rispetto a controlli particolari.

Ad esempio, se lo stato di conformità di una risorsa cambia da `FAILED` a `PASSED` per un particolare controllo, Security Hub CSPM non genera nuovi risultati. Invece, Security Hub CSPM aggiorna i risultati esistenti per il controllo e la risorsa. Nel risultato, Security Hub CSPM modifica il valore del campo compliance status (`Compliance.Status`) in. `PASSED` Security Hub CSPM aggiorna anche i valori per i campi aggiuntivi in modo da riflettere i risultati del controllo, ad esempio l'etichetta di gravità, lo stato del flusso di lavoro e i timestamp che indicano quando Security Hub CSPM ha eseguito il controllo più di recente e aggiornato il risultato.

Quando riporta le modifiche allo stato di conformità, Security Hub CSPM potrebbe aggiornare uno dei seguenti campi in un risultato di controllo:

- `Compliance.Status`— Il nuovo stato di conformità della risorsa per il controllo specificato.
- `FindingProviderFields.Severity.Label`— La nuova rappresentazione qualitativa della gravità del risultato, ad esempio `LOWMEDIUM`, o`HIGH`.
- `FindingProviderFields.Severity.Original`— La nuova rappresentazione quantitativa della gravità del risultato, ad esempio `0` per una risorsa conforme.
- `FirstObservedAt`— Data dell'ultima modifica dello stato di conformità della risorsa.
- `LastObservedAt`— L'ultima volta che Security Hub CSPM ha eseguito il controllo di sicurezza per il controllo e la risorsa specificati.
- `ProcessedAt`— Quando Security Hub CSPM ha recentemente iniziato a elaborare la scoperta.
- `ProductFields.PreviousComplianceStatus`— Lo stato di conformità precedente (`Compliance.Status`) della risorsa per il controllo specificato.
- `UpdatedAt`— Quando Security Hub CSPM ha aggiornato l'ultima volta la scoperta.
- `Workflow.Status`— Lo stato dell'indagine sul risultato, in base al nuovo stato di conformità della risorsa per il controllo specificato.

L'aggiornamento di un campo da parte di Security Hub CSPM dipende principalmente dai risultati dell'ultimo controllo di sicurezza per il controllo e la risorsa applicabili. Ad esempio, se lo stato di conformità di una risorsa cambia da `PASSED` a `FAILED` per un particolare controllo, Security Hub CSPM modifica lo stato del flusso di lavoro del risultato in. `NEW` Per tenere traccia degli aggiornamenti dei singoli risultati, puoi fare riferimento alla cronologia di un risultato. Per dettagli sui singoli campi dei risultati, consulta AWSSecurity Finding Format (ASFF).

In alcuni casi, Security Hub CSPM genera nuovi risultati per i controlli successivi tramite un controllo, invece di aggiornare i risultati esistenti. Questo può verificarsi se c'è un problema con la AWS Config regola che supporta un controllo. In tal caso, Security Hub CSPM archivia i risultati esistenti e genera un nuovo risultato per ogni controllo. Nelle nuove scoperte, lo stato di conformità è `NOT_AVAILABLE` e lo stato del record è. `ARCHIVED` Dopo aver risolto il problema con la AWS Config regola, Security Hub CSPM genera nuovi risultati e inizia ad aggiornarli per tenere traccia delle successive modifiche allo stato di conformità delle singole risorse.

Oltre a generare e aggiornare i risultati di controllo, Security Hub CSPM archivia automaticamente i risultati di controllo che soddisfano determinati criteri. Security Hub CSPM archivia un risultato se il controllo è disabilitato, la risorsa specificata viene eliminata o la risorsa specificata non esiste

più. Una risorsa potrebbe non esistere più perché il servizio associato non viene più utilizzato. Più specificamente, Security Hub CSPM archivia automaticamente un risultato di controllo se il risultato soddisfa uno dei seguenti criteri:

- Il risultato non viene aggiornato da 3-5 giorni. Tieni presente che l'archiviazione basata su questo periodo di tempo viene effettuata con la massima diligenza possibile e non è garantita.
- La AWS Config valutazione associata restituita `NOT_APPLICABLE` per lo stato di conformità della risorsa specificata.

Per determinare se un risultato è archiviato, è possibile fare riferimento al campo record state (`RecordState`) del risultato. Se un risultato è archiviato, il valore di questo campo è. `ARCHIVED`

Security Hub CSPM archivia i risultati di controllo archiviati per 30 giorni. Dopo 30 giorni, i risultati scadono e Security Hub CSPM li elimina definitivamente. Per determinare se un risultato di controllo archiviato è scaduto, Security Hub CSPM basa il calcolo sul valore del `UpdatedAt` campo del risultato.

Per archiviare i risultati di controllo archiviati per più di 30 giorni, puoi esportare i risultati in un bucket S3. Puoi farlo utilizzando un'azione personalizzata con una EventBridge regola Amazon. Per ulteriori informazioni, consulta Utilizzo EventBridge per la risposta e la correzione automatiche.

> **Note**
>
> Prima del 3 luglio 2025, Security Hub CSPM generava e aggiornava i risultati del controllo in modo diverso quando lo stato di conformità di una risorsa cambiava rispetto a un controllo. In precedenza, Security Hub CSPM creava un nuovo risultato di controllo e archiviava il risultato esistente per una risorsa. Pertanto, potreste avere più risultati archiviati per un particolare controllo e risorsa fino alla scadenza di tali risultati (dopo 30 giorni).

Automazione e soppressione dei risultati del controllo

È possibile utilizzare le regole di automazione CSPM di Security Hub per aggiornare o eliminare risultati di controllo specifici. Se si elimina un risultato, è possibile continuare ad accedervi. Tuttavia, la soppressione indica che ritenete che non sia necessaria alcuna azione per risolvere il problema.

Sopprimendo i risultati, è possibile ridurre il rumore di ricerca. Ad esempio, è possibile sopprimere i risultati dei controlli generati negli account di test. In alternativa, è possibile sopprimere i risultati

relativi a risorse specifiche. Per ulteriori informazioni sull'aggiornamento o la soppressione automatica dei risultati, consulta. Comprensione delle regole di automazione in Security Hub CSPM

Le regole di automazione sono appropriate quando si desidera aggiornare o eliminare risultati di controllo specifici. Tuttavia, se un controllo non è pertinente alla tua organizzazione o al tuo caso d'uso, ti consigliamo di disabilitarlo. Se disabiliti un controllo, Security Hub CSPM non esegue controlli di sicurezza per esso e non ti viene addebitato alcun costo.

Dettagli sulla conformità per i risultati del controllo

Nei risultati generati dai controlli di sicurezza, l'oggetto Compliance e i campi del AWS Security Finding Format (ASFF) forniscono dettagli sulla conformità per le singole risorse controllate da un controllo. Ciò include le seguenti informazioni:

- `AssociatedStandards`— Gli standard abilitati in cui è abilitato il controllo.
- `RelatedRequirements`— I relativi requisiti per il controllo in tutti gli standard abilitati. Questi requisiti derivano da framework di sicurezza di terze parti per il controllo, come il Payment Card Industry Data Security Standard (PCI DSS) o lo standard NIST SP 800-171 Revision 2.
- `SecurityControlId`— L'identificatore per il controllo attraverso gli standard supportati da Security Hub CSPM.
- `Status`— Il risultato del controllo più recente eseguito da Security Hub CSPM per il controllo. I risultati dei controlli precedenti vengono conservati nella cronologia del risultato.
- `StatusReasons`— Un array che elenca i motivi del valore specificato dal `Status` campo. Per ogni motivo, sono inclusi un codice motivo e una descrizione.

La tabella seguente elenca i codici dei motivi e le descrizioni che un risultato potrebbe includere nell'`StatusReasons`array. Le fasi di correzione variano in base al controllo che ha generato un risultato con un codice motivo specificato. Per rivedere le linee guida per la riparazione di un controllo, fare riferimento a. Riferimento di controllo per Security Hub CSPM

Codice di motivo	Compliance status (Stato di conformità)	Description
`CLOUDTRAIL_METRIC_FILTER_NOT_VALID`	`FAILED`	Il CloudTrail percorso multiregionale non dispone di un filtro metrico valido.

Codice di motivo	Compliance status (Stato di conformità)	Description
`CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT`	`FAILED`	I filtri metrici non sono presenti per il percorso multiregionale. CloudTrail
`CLOUDTRAIL_MULTI_REGION_NOT_PRESENT`	`FAILED`	L'account non dispone di un CloudTrail percorso multiregionale con la configurazione richiesta.
`CLOUDTRAIL_REGION_INVAILD`	`WARNING`	Multi-Region CloudTrail i sentieri non si trovano nella regione corrente.
`CLOUDWATCH_ALARM_ACTIONS_NOT_VALID`	`FAILED`	Non sono presenti operazioni di allarme valide.
`CLOUDWATCH_ALARMS_NOT_PRESENT`	`FAILED`	CloudWatch gli allarmi non esistono nell'account.
`CONFIG_ACCESS_DENIED`	`NOT_AVAILABLE` AWS Configlo stato è `ConfigError`	AWS Configaccesso negato. Verifica che AWS Config sia abilitato e che siano state concesse autorizzazioni sufficienti.
`CONFIG_EVALUATIONS_EMPTY`	`PASSED`	AWS Configha valutato le tue risorse in base alla regola. La regola non si applicava alle AWS risorse incluse nel suo ambito, le risorse specificate sono state eliminate o i risultati della valutazione sono stati eliminati.

Codice di motivo	Compliance status (Stato di conformità)	Description
`CONFIG_RECORDER_CUSTOM_ROLE`	`FAILED`(per Config.1)	Il AWS Config registratore utilizza un ruolo IAM personalizzato anziché il ruolo AWS Config collegato al servizio e il parametro `includeConfigServiceLinkedRoleCheck` personalizzato per Config.1 non è impostato su. `false`
`CONFIG_RECORDER_DISABLED`	`FAILED`(per) Config.1	AWS Confignon è abilitato con il registratore di configurazione acceso.
`CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES`	`FAILED`(per Config.1)	AWS Confignon registra tutti i tipi di risorse che corrispondono ai controlli CSPM di Security Hub abilitati. Attiva la registrazione per le seguenti risorse:. *`Resources that aren't being recorded`*

Codice di motivo	Compliance status (Stato di conformità)	Description
`CONFIG_RETURNS_NOT_APPLICABLE`	`NOT_AVAILABLE`	Lo stato di conformità è `NOT_AVAILABLE` dovuto al fatto che è stato AWS Config restituito lo stato Non applicabile. AWS Configgnon fornisce il motivo dello stato. Di seguito sono riportati alcuni possibili motivi dello stato Non applicabile: • La risorsa è stata rimossa dall'ambito della AWS Config regola. • La AWS Config regola è stata eliminata. • La risorsa è stata eliminata. • La logica della AWS Config regola può generare lo stato Non applicabile.

Codice di motivo	Compliance status (Stato di conformità)	Description
`CONFIG_RULE_EVALUATION_ERROR`	`NOT_AVAILABLE` AWS Configlo stato è `ConfigError`	Questo codice motivo viene utilizzato per diversi tipi di errori di valutazione. La descrizione fornisce le informazioni sul motivo specifico. Il tipo di errore può essere uno dei seguenti: • Impossibilità di eseguire la valutazione a causa della mancanza di autorizzazioni. La descrizione fornisce l'autorizzazione specifica mancante. • Valore mancante o non valido per un parametro. La descrizione fornisce il parametro e i requisiti per il valore del parametro. • Errore durante la lettura di un bucket S3. La descrizione identifica il bucket e fornisce l'errore specifico. • Un AWS abbonamento mancante. • Timeout generale sulla valutazione. • Un account sospeso.
`CONFIG_RULE_NOT_FOUND`	`NOT_AVAILABLE` AWS Configlo stato è `ConfigError`	La AWS Config regola è in fase di creazione.

Codice di motivo	Compliance status (Stato di conformità)	Description
`INTERNAL_SERVICE_ERROR`	`NOT_AVAILABLE`	Si è verificato un errore sconosciuto.
`LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE`	`FAILED`	Security Hub CSPM non è in grado di eseguire un controllo rispetto a un runtime Lambda personalizzato.
`S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION`	`WARNING`	Il risultato è in uno `WARNING` stato perché il bucket S3 associato a questa regola si trova in una regione o in un account diverso. Questa regola non supporta controlli tra regioni o account. È consigliabile disabilitare questo controllo in questa regione o account. Esegui solo nella regione o nell'account in cui si trova la risorsa.
`SNS_SUBSCRIPTION_NOT_PRESENT`	`FAILED`	I filtri metrici CloudWatch Logs non dispongono di un abbonamento Amazon SNS valido.

Codice di motivo	Compliance status (Stato di conformità)	Description
SNS_TOPIC_CROSS_ACCOUNT	WARNING	Il risultato è in uno stato. WARNING L'argomento SNS associato a questa regola è di proprietà di un account diverso. L'account corrente non è in grado di ottenere le informazioni sull'abbonamento. L'account proprietario dell'argomento SNS deve concedere all'account corrente l'sns:ListSubscriptionsByTopic autorizzazione per l'argomento SNS.
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	Il risultato è in uno WARNING stato in cui l'argomento SNS associato a questa regola si trova in una regione o in un account diverso. Questa regola non supporta controlli tra regioni o account. È consigliabile disabilitare questo controllo in questa regione o account. Esegui solo nella regione o nell'account in cui si trova la risorsa.
SNS_TOPIC_INVALID	FAILED	L'argomento SNS associato a questa regola non è valido.
THROTTLING_ERROR	NOT_AVAILABLE	L'operazione API pertinente ha superato il limite consentito.

ProductFields dettagli relativi ai risultati del controllo

Nei risultati generati dai controlli di sicurezza per i controlli, l'ProductFieldsattributo del AWS Security Finding Format (ASFF) può includere i seguenti campi.

`ArchivalReasons:0/Description`

Descrive perché Security Hub CSPM ha archiviato un risultato.

Ad esempio, Security Hub CSPM archivia i risultati esistenti quando si disabilita un controllo o uno standard oppure si abilitano o disabilitano i risultati del controllo consolidato.

`ArchivalReasons:0/ReasonCode`

Specifica il motivo per cui Security Hub CSPM ha archiviato un risultato.

Ad esempio, Security Hub CSPM archivia i risultati esistenti quando si disabilita un controllo o uno standard oppure si abilitano o disabilitano i risultati del controllo consolidato.

`PreviousComplianceStatus`

Lo stato di conformità precedente (`Compliance.Status`) della risorsa per il controllo specificato, a partire dall'aggiornamento più recente del risultato. Se lo stato di conformità della risorsa non è cambiato durante l'aggiornamento più recente, questo valore è uguale al valore del `Compliance.Status` campo del risultato. Per un elenco di possibili valori, consulta Valutazione dello stato di conformità e dello stato di controllo.

`StandardsGuideArn` o `StandardsArn`

L'ARN dello standard associato al controllo.

Per lo standard CIS AWS Foundations Benchmark, il campo è. `StandardsGuideArn` Per gli standard PCI DSS e AWS Foundational Security Best Practices, il campo è. `StandardsArn`

Questi campi vengono rimossi a favore di `Compliance.AssociatedStandards` se si abilitano i risultati di controllo consolidati.

`StandardsGuideSubscriptionArn` o `StandardsSubscriptionArn`

L'ARN dell'abbonamento dell'account allo standard.

Per lo standard CIS AWS Foundations Benchmark, il campo è. `StandardsGuideSubscriptionArn` Per gli standard PCI DSS e AWS Foundational Security Best Practices, il campo è. `StandardsSubscriptionArn`

Questi campi vengono rimossi se si abilitano i risultati del controllo consolidato.

`RuleId` o `ControlId`

L'identificatore del controllo.

Per la versione 1.2.0 dello standard AWS CIS Foundations Benchmark, il campo è. `RuleId` Per altri standard, comprese le versioni successive dello standard CIS AWS Foundations Benchmark, il campo è. `ControlId`

Questi campi vengono rimossi a favore di `Compliance.SecurityControlId` se si abilitano i risultati di controllo consolidati.

`RecommendationUrl`

L'URL per le informazioni sulla correzione del controllo. Questo campo viene rimosso a favore di `Remediation.Recommendation.Url` se si abilitano i risultati del controllo consolidato.

`RelatedAWSResources:0/name`

Il nome della risorsa associata al risultato.

`RelatedAWSResource:0/type`

Il tipo di risorsa associata al controllo.

`StandardsControlArn`

L'ARN del controllo. Questo campo viene rimosso se si abilitano i risultati del controllo consolidato.

`aws/securityhub/ProductName`

Per i risultati del controllo, il nome del prodotto è`Security Hub`.

`aws/securityhub/CompanyName`

Per i risultati del controllo, il nome dell'azienda è`AWS`.

`aws/securityhub/annotation`

Una descrizione del problema rilevato dal controllo.

`aws/securityhub/FindingId`

L'identificatore del risultato.

Questo campo non fa riferimento a uno standard se si abilitano i risultati di controllo consolidati.

Livelli di gravità per i risultati del controllo

La gravità assegnata a un controllo CSPM di Security Hub indica l'importanza del controllo. La gravità di un controllo determina l'etichetta di gravità assegnata ai risultati del controllo.

Criteri di gravità

La gravità di un controllo è determinata sulla base di una valutazione dei seguenti criteri:

- Quanto è difficile per un autore di minacce sfruttare la debolezza della configurazione associata al controllo? La difficoltà è determinata dal livello di sofisticazione o complessità necessario per utilizzare la vulnerabilità per realizzare uno scenario di minaccia.
- Quanto è probabile che la debolezza porti a una compromissione delle vostre Account AWS o delle vostre risorse? Una compromissione delle vostre Account AWS risorse significa che la riservatezza, l'integrità o la disponibilità dei dati o dell'AWSinfrastruttura vengono danneggiate in qualche modo. La probabilità di compromissione indica la probabilità che lo scenario di minaccia comporti un'interruzione o una violazione delle tue o delle tue Servizi AWS risorse.

Ad esempio, consideriamo i seguenti punti deboli della configurazione:

- Le chiavi di accesso utente non vengono ruotate ogni 90 giorni.
- La chiave utente root IAM esiste.

Entrambi i punti deboli sono ugualmente difficili da sfruttare per un avversario. In entrambi i casi, l'avversario può utilizzare il furto di credenziali o qualche altro metodo per acquisire una chiave utente. Possono quindi utilizzarlo per accedere alle tue risorse in modo non autorizzato.

Tuttavia, la probabilità di una compromissione è molto più elevata se l'autore della minaccia acquisisce la chiave di accesso dell'utente root, in quanto ciò gli offre un accesso maggiore. Di conseguenza, la vulnerabilità della chiave dell'utente root ha una gravità maggiore.

La gravità non tiene conto della criticità della risorsa sottostante. La criticità è il livello di importanza delle risorse associate alla scoperta. Ad esempio, una risorsa associata a un'applicazione mission critical è più importante di una associata a test non di produzione. Per acquisire informazioni sulla criticità delle risorse, utilizzate il `Criticality` campo del AWS Security Finding Format (ASFF).

La tabella seguente associa la difficoltà di sfruttamento e la probabilità di compromissione alle etichette di sicurezza.

	Un compromesso è altamente probabile	Compromesso probabile	Compromesso improbabile	Compromesso altamente improbabile
Molto facile da sfruttare	Critica	Critica	Elevata	Media
Un po' facile da sfruttare	Critica	Elevata	Media	Media
Un po' difficile da sfruttare	Elevata	Media	Media	Bassa
Molto difficile da sfruttare	Media	Media	Bassa	Bassa

Definizioni di gravità

Le etichette di gravità sono definite come segue.

Critico: il problema deve essere risolto immediatamente per evitare che si aggravi.

Ad esempio, un bucket S3 aperto è considerato un risultato di gravità critica. Poiché sono così tanti gli autori delle minacce che cercano i bucket S3 aperti, è probabile che i dati contenuti nei bucket S3 esposti vengano scoperti e consultati da altri.

In generale, le risorse accessibili al pubblico sono considerate problemi di sicurezza critici. È necessario trattare i risultati critici con la massima urgenza. È inoltre necessario considerare la criticità della risorsa.

Alto: il problema deve essere affrontato come priorità a breve termine.

Ad esempio, se un gruppo di sicurezza VPC predefinito è aperto al traffico in entrata e in uscita, viene considerato ad alta severità. È piuttosto facile per un autore di minacce compromettere un VPC utilizzando questo metodo. È anche probabile che l'autore della minaccia sia in grado di interrompere o esfiltrare le risorse una volta inserite nel VPC.

Security Hub CSPM consiglia di considerare un rilevamento di elevata gravità come una priorità a breve termine. È necessario adottare misure correttive immediate. È inoltre necessario considerare la criticità della risorsa.

Medio: la questione dovrebbe essere affrontata come priorità a medio termine.

Ad esempio, la mancanza di crittografia per i dati in transito è considerata una rilevazione di gravità media. È necessario un sofisticato attacco man-in-the-middle per sfruttare questa debolezza. In altre parole, è piuttosto difficile. È probabile che alcuni dati vengano compromessi se lo scenario di minaccia ha esito positivo.

Security Hub CSPM consiglia di esaminare la risorsa implicata il prima possibile. È inoltre necessario considerare la criticità della risorsa.

Basso: il problema non richiede di per sé un'azione.

Ad esempio, la mancata raccolta di informazioni forensi è considerata di bassa gravità. Questo controllo può aiutare a prevenire future compromessi, ma l'assenza di analisi forensi non porta direttamente a un compromesso.

Non è necessario agire immediatamente sugli esiti di bassa gravità, ma possono fornire un contesto quando li si correla con altri problemi.

Informativo: non è stato rilevato alcun punto debole nella configurazione.

In altre parole, lo stato è `PASSEDWARNING`, o`NOT AVAILABLE`.

Non vi è alcuna azione consigliata. I risultati informativi aiutano i clienti a dimostrare di essere conformi.

Valutazione dello stato di conformità e dello stato di controllo

Il `Compliance.Status` campo del AWS Security Finding Format descrive il risultato di un risultato di controllo. AWSSecurity Hub CSPM utilizza lo stato di conformità dei risultati del controllo per determinare lo stato di controllo generale. Lo stato del controllo viene visualizzato nella pagina dei dettagli di un controllo sulla console Security Hub CSPM.

Valutazione dello stato di conformità dei risultati del Security Hub CSPM

Allo stato di conformità per ogni risultato viene assegnato uno dei seguenti valori:

- `PASSED`— Indica che il controllo ha superato il controllo di sicurezza relativo al risultato. Questo imposta automaticamente il Security Hub CSPM `Workflow.Status` su. `RESOLVED`
- `FAILED`— Indica che il controllo non ha superato il controllo di sicurezza relativo al risultato.

- `WARNING`— Indica che Security Hub CSPM non è in grado di determinare se la risorsa si trova in uno stato `PASSED` o`FAILED`. Ad esempio, la registrazione AWS Config delle risorse non è attivata per il tipo di risorsa corrispondente.
- `NOT_AVAILABLE`— Indica che il controllo non può essere completato perché un server ha avuto un errore, la risorsa è stata eliminata o il risultato della AWS Config valutazione sì`NOT_APPLICABLE`. Se il risultato della AWS Config valutazione è stato`NOT_APPLICABLE`, Security Hub CSPM archivia automaticamente il risultato.

Se lo stato di conformità di un risultato cambia `PASSED` da`FAILED`, o`WARNING`, ed `Workflow.Status` era uno o`NOT_AVAILABLE`, o, `NOTIFIED` o`RESOLVED`, Security Hub CSPM cambia `Workflow.Status` automaticamente in. `NEW`

Se non disponi di risorse corrispondenti a un controllo, Security Hub CSPM produce un `PASSED` risultato a livello di account. Se hai una risorsa corrispondente a un controllo ma poi la elimini, Security Hub CSPM crea un `NOT_AVAILABLE` risultato e lo archivia immediatamente. Dopo 18 ore, ricevi un `PASSED` risultato perché non hai più risorse corrispondenti al controllo.

Determinare lo stato di controllo dallo stato di conformità

Security Hub CSPM ricava uno stato di controllo generale dallo stato di conformità dei risultati del controllo. Nel determinare lo stato del controllo, Security Hub CSPM ignora i risultati con un `RecordState` di `ARCHIVED` e i risultati con un di. `Workflow.Status` `SUPPRESSED`

Allo stato del controllo viene assegnato uno dei seguenti valori:

- Passato: indica che tutti i risultati hanno uno stato di conformità pari a`PASSED`.
- Non riuscito: indica che almeno un risultato ha uno stato di conformità pari a`FAILED`.
- Sconosciuto: indica che almeno un risultato ha uno stato di conformità pari a `WARNING` o`NOT_AVAILABLE`. Nessun risultato ha uno stato di conformità pari a`FAILED`.
- Nessun dato: indica che non ci sono risultati per il controllo. Ad esempio, un controllo appena abilitato ha questo stato fino a quando Security Hub CSPM non inizia a generare i relativi risultati. Un controllo ha questo stato anche se tutti i risultati sono `SUPPRESSED` o non sono disponibili nella versione corrente. Regione AWS
- Disabilitato: indica che il controllo è disabilitato nell'account e nella regione correnti. Al momento non vengono eseguiti controlli di sicurezza per questo controllo nell'account e nella regione correnti. Tuttavia, i risultati di un controllo disattivato possono avere un valore per lo stato di conformità fino a 24 ore dopo la disabilitazione.

Per un account amministratore, lo stato di controllo riflette lo stato di controllo dell'account amministratore e degli account membro. In particolare, lo stato generale di un controllo appare come Non riuscito se il controllo presenta uno o più risultati non riusciti nell'account amministratore o in uno degli account dei membri. Se è stata impostata una regione di aggregazione, lo stato di controllo nella regione di aggregazione riflette lo stato di controllo nella regione di aggregazione e nelle regioni collegate. In particolare, lo stato generale di un controllo appare come Non riuscito se il controllo presenta uno o più risultati non riusciti nella regione di aggregazione o in una delle regioni collegate.

Security Hub CSPM genera in genere lo stato di controllo iniziale entro 30 minuti dalla prima visita alla pagina di riepilogo o alla pagina degli standard di sicurezza sulla console CSPM di Security Hub. È necessario che la registrazione AWS Config delle risorse sia configurata per visualizzare lo stato del controllo. Dopo la prima generazione degli stati di controllo, Security Hub CSPM aggiorna gli stati di controllo ogni 24 ore in base ai risultati delle 24 ore precedenti. Un timestamp nella pagina dei dettagli del controllo indica quando lo stato del controllo è stato aggiornato l'ultima volta.

> **Note**
>
> Dopo aver abilitato un controllo per la prima volta, possono essere necessarie fino a 24 ore per generare gli stati di controllo nelle regioni della Cina e nelAWS GovCloud (US) Region.

Calcolo dei punteggi di sicurezza

Nella console AWS Security Hub CSPM, la pagina Riepilogo e la pagina Controlli visualizzano un punteggio di sicurezza riepilogativo per tutti gli standard abilitati. Nella pagina degli standard di sicurezza, Security Hub CSPM mostra anche un punteggio di sicurezza compreso tra 0 e 100 percento per ogni standard abilitato.

Quando si attiva Security Hub CSPM per la prima volta, Security Hub CSPM calcola il punteggio di sicurezza riepilogativo e i punteggi di sicurezza standard entro 30 minuti dalla prima visita alla pagina Riepilogo o agli standard di sicurezza sulla console. I punteggi vengono generati solo per gli standard abilitati quando visiti tali pagine sulla console. Inoltre, la registrazione AWS Config delle risorse deve essere configurata affinché i punteggi vengano visualizzati. Il punteggio di sicurezza riepilogativo è la media dei punteggi di sicurezza standard. Per esaminare un elenco degli standard attualmente abilitati, è possibile utilizzare il GetEnabledStandards funzionamento dell'API CSPM Security Hub.

Dopo la prima generazione del punteggio, Security Hub CSPM aggiorna i punteggi di sicurezza ogni 24 ore. Security Hub CSPM mostra un timestamp per indicare quando un punteggio di sicurezza è

stato aggiornato l'ultima volta. Tieni presente che possono essere necessarie fino a 24 ore per la prima generazione dei punteggi di sicurezza nelle regioni della Cina e. AWS GovCloud (US) Regions

Se attivi i risultati di controllo consolidati, l'aggiornamento dei punteggi di sicurezza può richiedere fino a 24 ore. Inoltre, l'attivazione di una nuova regione di aggregazione o l'aggiornamento delle regioni collegate reimposta i punteggi di sicurezza esistenti. Il Security Hub CSPM può impiegare fino a 24 ore per generare nuovi punteggi di sicurezza che includono i dati delle regioni aggiornate.

Metodo di calcolo dei punteggi di sicurezza

I punteggi di sicurezza rappresentano la proporzione dei controlli superati rispetto ai controlli abilitati. Il punteggio viene visualizzato come percentuale arrotondata per eccesso o per difetto al numero intero più vicino.

Security Hub CSPM calcola un punteggio di sicurezza riepilogativo per tutti gli standard abilitati. Security Hub CSPM calcola anche un punteggio di sicurezza per ogni standard abilitato. Ai fini del calcolo del punteggio, i controlli abilitati includono i controlli con lo stato Passato , Non riuscito e Sconosciuto. I controlli con lo stato Nessun dato sono esclusi dal calcolo del punteggio.

Security Hub CSPM ignora i risultati archiviati e soppressi nel calcolo dello stato del controllo. Ciò può influire sui punteggi di sicurezza. Ad esempio, se si eliminano tutti i risultati non riusciti di un controllo, il relativo stato diventa Passato, il che a sua volta può migliorare i punteggi di sicurezza. Per ulteriori informazioni sullo stato del controllo, vedereValutazione dello stato di conformità e dello stato di controllo.

Esempio di punteggio:

Standard	Controlli superati	Controlli non riusciti	Controlli sconosciuti	Punteggio standard
AWS Best practice fondamentali per la sicurezza v1.0.0	168	22	0	88%
CIS AWS Foundations	8	29	0	22%

Standard	Controlli superati	Controlli non riusciti	Controlli sconosciuti	Punteggio standard
Benchmark v1.4.0				
CIS AWS Foundations Benchmark v1.2.0	6	35	0	15%
Pubblicazione speciale del NIST 800-53 Revisione 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

Nel calcolo del punteggio di sicurezza riepilogativo, Security Hub CSPM conta ogni controllo una sola volta tra gli standard. Ad esempio, se hai abilitato un controllo che si applica a tre standard abilitati, viene conteggiato come un solo controllo abilitato ai fini del punteggio.

In questo esempio, sebbene il numero totale di controlli abilitati tra gli standard abilitati sia 528, Security Hub CSPM conta ogni controllo univoco una sola volta ai fini del punteggio. Il numero di controlli univoci abilitati è probabilmente inferiore a 528. Se assumiamo che il numero di controlli univoci abilitati sia 515 e il numero di controlli univoci superati sia 357, il punteggio di riepilogo è del 69%. Questo punteggio viene calcolato dividendo il numero di controlli univoci passati per il numero di controlli univoci abilitati.

Potresti avere un punteggio di riepilogo diverso dal punteggio di sicurezza standard, anche se hai abilitato solo uno standard nel tuo account nella regione corrente. Ciò può verificarsi se hai effettuato l'accesso a un account amministratore e gli account membri hanno standard aggiuntivi o standard diversi abilitati. Ciò può verificarsi anche se stai visualizzando il punteggio della regione di aggregazione e nelle regioni collegate sono abilitati standard aggiuntivi o standard diversi.

Punteggi di sicurezza per gli account di amministratore

Se hai effettuato l'accesso a un account amministratore, il punteggio di sicurezza riepilogativo e i punteggi standard tengono conto degli stati di controllo nell'account amministratore e in tutti gli account membri.

Se lo stato di un controllo è Fallito anche in un solo account membro, tale stato è Non riuscito nell'account amministratore e influisce sui punteggi dell'account amministratore.

Se hai effettuato l'accesso a un account amministratore e stai visualizzando i punteggi in una regione di aggregazione, i punteggi di sicurezza tengono conto degli stati di controllo in tutti gli account membri e in tutte le regioni collegate.

Punteggi di sicurezza se hai impostato una regione di aggregazione

Se hai impostato un'aggregazione Regione AWS, il punteggio di sicurezza riepilogativo e i punteggi standard tengono conto degli stati di controllo complessivi
Regioni collegate.

Se lo stato di un controllo è Fallito anche in una sola regione collegata, il suo stato è Fallito nella regione di aggregazione e influisce sui punteggi della regione di aggregazione.

Se hai effettuato l'accesso a un account amministratore e stai visualizzando i punteggi in una regione di aggregazione, i punteggi di sicurezza tengono conto degli stati di controllo in tutti gli account membri e in tutte le regioni collegate.

Categorie di controllo in Security Hub CSPM

A ogni controllo viene assegnata una categoria. La categoria di un controllo riflette la funzione di protezione a cui si applica il controllo.

Il valore della categoria contiene la categoria, la sottocategoria all'interno della categoria e, facoltativamente, un classificatore all'interno della sottocategoria. Esempio:

- Identifica > Inventario
- Proteggi > Protezione dei dati > Crittografia dei dati in transito

Di seguito sono riportate le descrizioni delle categorie, sottocategorie e classificatori disponibili.

Identificazione

Sviluppare le conoscenze organizzative per gestire i rischi di sicurezza informatica per sistemi, risorse, dati e funzionalità.

Inventory

Il servizio ha implementato le strategie di tagging delle risorse corrette? Le strategie di tagging includono il proprietario della risorsa?

Quali risorse utilizza il servizio? Sono risorse approvate per questo servizio?

Hai visibilità sull'inventario approvato? Ad esempio, utilizzi servizi come Amazon EC2 Systems Manager e Service Catalog?

Registrazione dei log

Hai abilitato in modo sicuro tutte le registrazioni rilevanti per il servizio? Alcuni esempi di file di log includono:

- Log di flusso Amazon VPC
- Log di accesso per Elastic Load Balancing
- CloudFront Registri Amazon
- CloudWatch Registri Amazon
- Registrazione di Amazon Relational Database Service
- Log di indicizzazione lenti di Amazon OpenSearch Service
- X-Ray tracciamento
- Servizio di directory AWSregistri
- AWS Configarticoli
- Snapshot

Protezione

Sviluppare e implementare le misure di sicurezza appropriate per garantire la fornitura di servizi di infrastruttura critica e procedure di codifica sicure.

Gestione sicura degli accessi

Il servizio utilizza pratiche con privilegi minimi nelle sue politiche IAM o in materia di risorse?

Le password e i segreti sono sufficientemente complessi? Sono ruotati in modo appropriato?

Il servizio utilizza l'autenticazione a più fattori (MFA)?

Il servizio evita l'utente root?

I criteri basati sulle risorse consentono l'accesso pubblico?

Configurazione di rete sicura

Il servizio evita l'accesso alla rete remota pubblico e non sicuro?

Il servizio utilizza correttamente i VPC? Ad esempio, i processi devono essere eseguiti in VPC?

Il servizio segmenta e isola correttamente le risorse sensibili?

Protezione dei dati

Crittografia dei dati inattivi: il servizio crittografa i dati inattivi?

Crittografia dei dati in transito: il servizio crittografa i dati in transito?

Integrità dei dati: il servizio convalida l'integrità dei dati?

Protezione dall'eliminazione dei dati: il servizio protegge i dati dall'eliminazione accidentale?

Gestione e utilizzo dei dati: utilizzi servizi come Amazon Macie per tracciare la posizione dei tuoi dati sensibili?

Protezione API

Il servizio viene utilizzato AWS PrivateLink per proteggere le operazioni dell'API del servizio?

Servizi di protezione

Sono in atto i servizi di protezione corretti? Forniscono la giusta quantità di copertura?

I servizi di protezione consentono di deviare gli attacchi e i compromessi diretti al servizio. Esempi di servizi di protezione AWS includonoAWS Control Tower,,AWS WAF, VantaAWS Shield Advanced, Secrets Manager, IAM Access Analyzer eAWS Resource Access Manager.

Sviluppo sicuro

Si utilizzano pratiche di codifica sicure?

Si evitano vulnerabilità quali la Top Ten Open Web Application Security Project (OWASP)?

Rilevamento

Sviluppare e implementare le attività appropriate per identificare il verificarsi di un evento di sicurezza informatica.

Servizi di rilevamento

- Sono disponibili i servizi di rilevamento corretti?
- Forniscono la giusta quantità di copertura?
- Esempi di servizi di AWS rilevamento includono Amazon GuardDuty, AWS Security Hub CSPM, Amazon Inspector, Amazon Detective, CloudWatch Amazon AWS IoT Device Defender Alarms e. AWS Trusted Advisor

Rispondi

Sviluppare e implementare le attività appropriate per intervenire in merito a un evento di sicurezza informatica rilevato.

Azioni di risposta

- Rispondi rapidamente agli eventi di sicurezza?
- Avete qualche risultato critico attivo o ad alta gravità?

Informatica forense

- È possibile acquisire in modo sicuro i dati forensi per il servizio? Ad esempio, acquisisci istantanee di Amazon EBS associate a risultati realmente positivi?
- Hai creato un account forense?

Ripristino

Sviluppare e implementare le attività appropriate per mantenere piani di resilienza e ripristinare eventuali funzionalità o servizi compromessi a causa di un evento di sicurezza informatica.

Resilienza

- La configurazione del servizio supporta failover agevoli, scalabilità elastica e disponibilità elevata?
- Sono stati stabiliti dei backup?

Revisione dei dettagli dei controlli in Security Hub CSPM

Selezionando un controllo nella pagina Controlli o nella pagina dei dettagli standard della console Security Hub CSPM si accede a una pagina con i dettagli del controllo.

La parte superiore della pagina dei dettagli del controllo indica lo stato del controllo. Lo stato del controllo riassume le prestazioni di un controllo in base allo stato di conformità dei risultati del controllo. Security Hub CSPM in genere genera lo stato di controllo iniziale entro 30 minuti dalla prima visita alla pagina di riepilogo o alla pagina degli standard di sicurezza sulla console Security Hub CSPM. Gli stati sono disponibili solo per i controlli abilitati quando si visitano tali pagine.

La pagina dei dettagli del controllo fornisce anche un'analisi dettagliata dello stato di conformità dei risultati del controllo nelle ultime 24 ore. Per ulteriori informazioni sullo stato del controllo e sullo stato di conformità, vedereValutazione dello stato di conformità e dello stato di controllo.

AWS Config la registrazione delle risorse deve essere configurata affinché venga visualizzato lo stato del controllo. Dopo la prima generazione degli stati di controllo, Security Hub CSPM aggiorna lo stato di controllo ogni 24 ore in base ai risultati delle 24 ore precedenti.

Gli account amministratore visualizzano uno stato di controllo aggregato tra l'account amministratore e gli account membri. Se hai impostato una regione di aggregazione, lo stato di controllo include i risultati di tutte le regioni collegate. Per ulteriori informazioni sullo stato del controllo, consultathe section called “Stato di conformità e stato di controllo”.

È inoltre possibile abilitare o disabilitare il controllo dalla pagina dei dettagli del controllo.

> **Note**
>
> Dopo l'attivazione di un controllo, possono essere necessarie fino a 24 ore per la generazione degli stati di primo controllo nelle regioni della Cina e. AWS GovCloud (US) Regions

La scheda Standard e requisiti elenca gli standard per i quali è possibile abilitare un controllo e i requisiti relativi al controllo previsti da diversi framework di conformità.

La scheda Controlli elenca i risultati attivi del controllo nelle ultime 24 ore. I risultati del controllo vengono generati e aggiornati quando Security Hub CSPM esegue i controlli di sicurezza per il controllo. L'elenco in questa scheda non include i risultati archiviati.

Per ogni risultato, l'elenco consente di accedere a dettagli quali lo stato di conformità e la risorsa correlata. È inoltre possibile impostare lo stato del flusso di lavoro di ogni risultato e inviare i risultati ad azioni personalizzate. Per ulteriori informazioni, consulta Revisione e gestione dei risultati del controllo.

Visualizzazione dei dettagli di un controllo

Scegli il tuo metodo di accesso preferito e segui questi passaggi per esaminare i dettagli di un controllo. I dettagli si riferiscono all'account corrente e alla regione e includono quanto segue:

- Il titolo e la descrizione del controllo.
- Un collegamento alle linee guida per porre rimedio ai risultati del controllo non riusciti.
- La severità del controllo.
- Lo stato del controllo.

Sulla console, puoi anche visualizzare un elenco dei risultati recenti relativi al controllo. Per eseguire questa operazione a livello di codice, puoi utilizzare il GetFindings funzionamento dell'API CSPM di Security Hub.

Security Hub CSPM console

1. Aprire la console CSPM di AWS Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Scegli Controlli nel pannello di navigazione.
3. Seleziona un controllo.

Security Hub CSPM API

1. Esegui `ListSecurityControlDefinitions` e fornisci uno o più ARN standard per ottenere un elenco di ID di controllo per quello standard. Per ottenere gli ARN standard, esegui. `DescribeStandards` Se non fornisci un ARN standard, questa API restituisce tutti gli ID di controllo CSPM di Security Hub. Questa API restituisce ID di controllo di sicurezza indipendenti dallo standard, non gli ID di controllo basati su standard esistenti prima di queste versioni di funzionalità.

   Esempio di richiesta:

```
{
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. Esegui BatchGetSecurityControls per ottenere dettagli su uno o più controlli nell'attuale Account AWS e Regione AWS.

   Esempio di richiesta:

```
{
    "SecurityControlIds": ["Config.1", "IAM.1"]
}
```

AWS CLI

1. Esegui il list-security-control-definitions comando e fornisci uno o più ARN standard per ottenere un elenco di ID di controllo. Per ottenere ARN standard, esegui il `describe-standards` comando. Se non si fornisce un ARN standard, questo comando restituisce tutti gli ID di controllo CSPM di Security Hub. Questo comando restituisce gli ID di controllo di sicurezza indipendenti dallo standard, non gli ID di controllo basati su standard esistenti prima di queste versioni di funzionalità.

```
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. Esegui il batch-get-security-controls comando per ottenere dettagli su uno o più controlli nell'attuale e. Account AWS Regione AWS

```
aws securityhub --region us-east-1 batch-get-security-controls --security-control-ids '["Config.1", "IAM.1"]'
```

Filtraggio e ordinamento dei controlli in Security Hub CSPM

Nella console AWS Security Hub CSPM, è possibile utilizzare la pagina Controlli per esaminare una tabella dei controlli disponibili nella versione corrente. Regione AWS L'eccezione è una regione di aggregazione. Se hai configurato una regione di aggregazione e accedi a tale regione, la console mostra i controlli disponibili nella regione di aggregazione o in una o più regioni collegate.

Per concentrarti su un sottoinsieme specifico di controlli, puoi ordinare e filtrare la tabella dei controlli. Le opzioni Filtra per accanto alla tabella possono aiutarti a concentrarti rapidamente su questi sottoinsiemi specifici:

- Tutti i controlli abilitati, ossia controlli abilitati in almeno uno standard abilitato.
- Tutti i controlli disattivati, ossia controlli disattivati in tutti gli standard.
- Tutti i controlli abilitati con uno stato di controllo specifico, ad esempio Non riuscito. L'opzione Nessun dato mostra solo i controlli per i quali attualmente non sono disponibili risultati. Per informazioni sullo stato dei controlli, consultaValutazione dello stato di conformità e dello stato di controllo.

Oltre alle opzioni Filtra per, è possibile filtrare la tabella inserendo i criteri di filtro nella casella Filtra controlli sopra la tabella. Ad esempio, puoi filtrare per ID di controllo o gravità.

Per impostazione predefinita, i controlli con stato Non riuscito vengono elencati per primi, in ordine decrescente per gravità. È possibile modificare l'ordinamento scegliendo un'intestazione di colonna diversa.

> **Tip**
>
> Se disponi di flussi di lavoro automatizzati basati sui risultati dei controlli, ti consigliamo di utilizzare i campi `SecurityControlId` o `SecurityControlArn` ASFF come filtri, anziché i campi `Title` o`Description`. Questi ultimi campi possono cambiare occasionalmente, mentre control ID e ARN sono identificatori statici.

Se hai effettuato l'accesso a un account amministratore CSPM di Security Hub, i controlli abilitati includono i controlli abilitati in almeno un account membro. Se hai configurato una regione di aggregazione, i controlli abilitati includono i controlli abilitati in almeno una regione collegata.

Se si seleziona l'opzione accanto a un controllo abilitato, viene visualizzato un pannello con gli standard in cui il controllo è attualmente abilitato. È inoltre possibile visualizzare gli standard in cui il controllo è attualmente disabilitato. Da questo pannello è possibile disattivare un controllo in tutti gli standard. Per ulteriori informazioni, consulta Disattivazione dei controlli in Security Hub CSPM. Per gli account amministratore, le informazioni nel pannello riflettono le impostazioni di tutti gli account membri.

Per recuperare un elenco di controlli a livello di codice, puoi utilizzare il ListSecurityControlDefinitions funzionamento dell'API CSPM Security Hub. Per recuperare i dettagli dei singoli controlli, usa l'operazione. BatchGetSecurityControls

Comprensione dei parametri di controllo in Security Hub CSPM

Alcuni controlli in AWS Security Hub CSPM utilizzano parametri che influiscono sulla modalità di valutazione del controllo. In genere, tali controlli vengono valutati in base ai valori dei parametri predefiniti da Security Hub CSPM. Tuttavia, per un sottoinsieme di questi controlli, è possibile modificare i valori dei parametri. Quando si modifica il valore di un parametro di controllo, Security Hub CSPM inizia a valutare il controllo rispetto al valore specificato. Se la risorsa alla base del controllo soddisfa il valore personalizzato, Security Hub CSPM genera un risultato. `PASSED` Se la risorsa non soddisfa il valore personalizzato, Security Hub CSPM genera un risultato. `FAILED`

Personalizzando i parametri di controllo, è possibile perfezionare le best practice di sicurezza consigliate e monitorate da Security Hub CSPM per allinearle ai requisiti aziendali e alle aspettative di sicurezza. Invece di eliminare i risultati relativi a un controllo, puoi personalizzare uno o più dei relativi parametri per ottenere risultati che soddisfino le tue esigenze di sicurezza.

Ecco alcuni esempi di casi d'uso per modificare i parametri di controllo e impostare valori personalizzati:

- [CloudWatch.16] — i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato

  È possibile specificare il periodo di conservazione.
- [IAM.7] — Le politiche relative alle password per gli utenti IAM devono avere configurazioni complesse

  È possibile specificare i parametri relativi alla sicurezza delle password.
- [EC2.18] — I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate

È possibile specificare quali porte sono autorizzate a consentire il traffico in entrata senza restrizioni.

- [Lambda.5] — Le funzioni VPC Lambda dovrebbero funzionare in più zone di disponibilità

  È possibile specificare il numero minimo di zone di disponibilità che produce un risultato superato.

Questa sezione descrive gli aspetti da considerare quando si modificano i parametri di controllo.

Effetto della modifica dei valori dei parametri di controllo

Quando si modifica il valore di un parametro, si attiva anche un nuovo controllo di sicurezza che valuta il controllo in base al nuovo valore. Security Hub CSPM genera quindi nuovi risultati di controllo in base al nuovo valore. Durante gli aggiornamenti periodici dei risultati di controllo, Security Hub CSPM utilizza anche il nuovo valore del parametro. Se modifichi i valori dei parametri per un controllo, ma non hai abilitato nessuno standard che includa il controllo, Security Hub CSPM non esegue alcun controllo di sicurezza utilizzando i nuovi valori. È necessario abilitare almeno uno standard pertinente per Security Hub CSPM per valutare il controllo in base al nuovo valore del parametro.

Un controllo può avere uno o più parametri personalizzabili. I tipi di dati possibili per ciascun parametro di controllo sono i seguenti:

- Booleano
- Double
- Enum
- EnumList
- Numero intero
- IntegerList
- Stringa
- StringList

I valori dei parametri personalizzati si applicano a tutti gli standard abilitati. Non puoi personalizzare i parametri per un controllo che non è supportato nella tua regione attuale. Per un elenco dei limiti regionali per i singoli controlli, consulta[Limiti regionali sui controlli CSPM di Security Hub](#).

Per alcuni controlli, i valori dei parametri accettabili devono rientrare in un intervallo specificato per essere validi. In questi casi, Security Hub CSPM fornisce l'intervallo accettabile.

Security Hub CSPM sceglie i valori dei parametri predefiniti e potrebbe occasionalmente aggiornarli. Dopo aver personalizzato un parametro di controllo, il suo valore continua a essere il valore specificato per il parametro, a meno che non venga modificato. In altre parole, il parametro interrompe il tracciamento degli aggiornamenti al valore CSPM predefinito di Security Hub, anche se il valore personalizzato del parametro corrisponde al valore predefinito corrente definito da Security Hub CSPM. Ecco un esempio del controllo [ACM.1] — Importato e i ACM-issued certificati devono essere rinnovati dopo un periodo di tempo specificato:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
    }
}
```

Nell'esempio precedente, il `daysToExpiration` parametro ha un valore personalizzato di`30`. Anche il valore predefinito corrente per questo parametro è`30`. Se Security Hub CSPM modifica il valore predefinito in`14`, il parametro in questo esempio non terrà traccia di tale modifica. Manterrà il valore di. `30`

Se desideri tenere traccia degli aggiornamenti al valore CSPM predefinito di Security Hub per un parametro, imposta il `ValueType` campo su `DEFAULT` anziché su. `CUSTOM` Per ulteriori informazioni, consulta Ripristino dei parametri di controllo predefiniti in un singolo account e regione.

Controlli che supportano parametri personalizzati

Per un elenco dei controlli di sicurezza che supportano parametri personalizzati, consulta la pagina Controlli della console Security Hub CSPM o il. Riferimento di controllo per Security Hub CSPM Per recuperare questo elenco a livello di codice, è possibile utilizzare l'operazione. ListSecurityControlDefinitions Nella risposta, l'`CustomizableProperties`oggetto indica quali controlli supportano parametri personalizzabili.

Revisione dei valori correnti dei parametri di controllo

Può essere utile conoscere il valore corrente di un parametro di controllo prima di modificarlo.

Puoi rivedere i valori correnti per i singoli parametri di controllo nel tuo account. Se si utilizza la configurazione centrale, l'amministratore delegato di AWS Security Hub CSPM può anche esaminare i valori dei parametri specificati in una politica di configurazione.

Scegliete il metodo preferito e seguite i passaggi per rivedere i valori correnti dei parametri di controllo.

Security Hub CSPM console

Per rivedere i valori correnti dei parametri di controllo (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel pannello di navigazione, scegli Controlli. Scegli un controllo.
3. Scegli la scheda Parametri. Questa scheda mostra i valori dei parametri correnti per il controllo.

Security Hub CSPM API

Per esaminare i valori correnti dei parametri di controllo (API)

Richiama l'BatchGetSecurityControlsAPI e fornisci uno o più ID di controllo di sicurezza o ARN. L'`Parameters`oggetto nella risposta mostra i valori dei parametri correnti per i controlli specificati.

Ad esempio, il AWS CLI comando seguente mostra i valori dei parametri correnti per `APIGatway.1`, `CloudWatch.15`, `eIAM.7`. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Scegliete il metodo preferito per visualizzare i valori dei parametri correnti in una politica di configurazione centrale.

Security Hub CSPM console

Per esaminare i valori correnti dei parametri di controllo in una politica di configurazione (console)

1. Aprire la console AWS Security Hub CSPM all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore CSPM di Security Hub delegato nella regione d'origine.
2. Nel pannello di navigazione, scegli Impostazioni e configurazione.
3. Nella scheda Criteri, seleziona il criterio di configurazione, quindi scegli Visualizza dettagli. Vengono quindi visualizzati i dettagli della politica, inclusi i valori dei parametri correnti.

Security Hub CSPM API

Per esaminare i valori correnti dei parametri di controllo in una politica di configurazione (API)

1. Richiama l'GetConfigurationPolicyAPI dall'account amministratore delegato nella regione principale.
2. Fornisci l'ARN o l'ID della politica di configurazione di cui desideri visualizzare i dettagli. La risposta include i valori dei parametri correnti.

Ad esempio, il AWS CLI comando seguente recupera i valori dei parametri di controllo correnti nella politica di configurazione specificata. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

I risultati del controllo includono anche i valori correnti dei parametri di controllo. InAWS Formato ASFF (Security Finding Format), questi valori vengono visualizzati nel `Parameters` campo dell'`Compliance`oggetto. Per esaminare i risultati sulla console Security Hub CSPM, scegli Risultati

nel riquadro di navigazione. Per esaminare i risultati a livello di codice, utilizza il GetFindings funzionamento dell'API CSPM di Security Hub.

Personalizzazione dei valori dei parametri di controllo

Le istruzioni per la personalizzazione dei parametri di controllo variano a seconda che si utilizzi o meno la configurazione centrale in AWS Security Hub CSPM. La configurazione centrale è una funzionalità che l'amministratore delegato di Security Hub CSPM può utilizzare per configurare le funzionalità CSPM di Security Hub tra account e unità organizzative (Regioni AWS OU).

Se l'organizzazione utilizza la configurazione centrale, l'amministratore delegato può creare politiche di configurazione che includono parametri di controllo personalizzati. Queste politiche possono essere associate agli account dei membri e alle unità organizzative gestite centralmente e hanno effetto nella regione di origine e in tutte le regioni collegate. L'amministratore delegato può anche designare uno o più account come autogestiti, il che consente al proprietario dell'account di configurare i propri parametri separatamente in ciascuna regione. Se l'organizzazione non utilizza la configurazione centrale, è necessario personalizzare i parametri di controllo separatamente in ogni account e regione.

Ti consigliamo di utilizzare la configurazione centrale perché consente di allineare i valori dei parametri di controllo nelle diverse parti dell'organizzazione. Ad esempio, tutti gli account di test potrebbero utilizzare determinati valori di parametro e tutti gli account di produzione potrebbero utilizzare valori diversi.

Personalizzazione dei parametri di controllo in più account e regioni

Se sei l'amministratore CSPM delegato di Security Hub per un'organizzazione che utilizza la configurazione centrale, scegli il tuo metodo preferito e segui i passaggi per personalizzare i parametri di controllo su più account e regioni.

Security Hub CSPM console

Per personalizzare i valori dei parametri di controllo in più account e regioni (console)

1. Aprire la console AWS Security Hub CSPM all'indirizzo. https://console.aws.amazon.com/securityhub/

   Assicurati di aver effettuato l'accesso alla regione di origine.
2. Nel pannello di navigazione, scegli Impostazioni e configurazione.

3. Scegliere la scheda Policy.
4. Per creare una nuova politica di configurazione che includa parametri personalizzati, scegli Crea politica. Per specificare parametri personalizzati in una politica di configurazione esistente, seleziona la politica, quindi scegli Modifica.

   Per creare una nuova politica di configurazione con valori dei parametri di controllo personalizzati

   1. Nella sezione Politica personalizzata, scegli gli standard e i controlli di sicurezza che desideri abilitare.
   2. Seleziona Personalizza i parametri di controllo.
   3. Seleziona un controllo, quindi specifica i valori personalizzati per uno o più parametri.
   4. Per personalizzare i parametri per più controlli, scegli Personalizza controllo aggiuntivo.
   5. Nella sezione Account, seleziona gli account o le unità organizzative a cui desideri applicare la policy.
   6. Scegli Next (Successivo).
   7. Scegli Crea policy e applica. Nella tua regione di origine e in tutte le regioni collegate, questa azione sovrascrive le impostazioni di configurazione esistenti degli account e delle unità organizzative associate a questa politica di configurazione. Gli account e le unità organizzative possono essere associati a una politica di configurazione tramite applicazione diretta o ereditarietà da un genitore.

   Per personalizzare i valori dei parametri di controllo in una politica di configurazione esistente

   1. Nella sezione Controlli, in Politica personalizzata, specifica i nuovi valori dei parametri personalizzati che desideri.
   2. Se è la prima volta che personalizzi i parametri di controllo in questa policy, seleziona Personalizza i parametri di controllo, quindi seleziona un controllo da personalizzare. Per personalizzare i parametri per ulteriori controlli, scegli Personalizza controllo aggiuntivo.
   3. Nella sezione Account, verifica gli account o le unità organizzative a cui desideri applicare la policy.
   4. Scegli Next (Successivo).
   5. Rivedi le modifiche e verifica che siano corrette. Al termine, scegli Salva politica e applica. Nella tua regione di origine e in tutte le regioni collegate, questa azione sovrascrive le impostazioni di configurazione esistenti degli account e delle unità organizzative associate

a questa politica di configurazione. Gli account e le unità organizzative possono essere associati a una politica di configurazione tramite applicazione diretta o ereditarietà da un genitore.

Security Hub CSPM API

Per personalizzare i valori dei parametri di controllo in più account e regioni (API)

Per creare una nuova politica di configurazione con valori dei parametri di controllo personalizzati

1. Richiama l'CreateConfigurationPolicyAPI dall'account amministratore delegato nella regione principale.
2. Per l'`SecurityControlCustomParameters`oggetto, fornisci l'identificatore di ogni controllo che desideri personalizzare.
3. Per l'`Parameters`oggetto, fornisci il nome di ogni parametro che desideri personalizzare. Per ogni parametro che personalizzi, fornisci `CUSTOM`Value`Type`. Per`Value`, fornisci il tipo di dati del parametro e il valore personalizzato. Il `Value` campo non può essere vuoto quando lo `ValueType` è`CUSTOM`. Se la richiesta omette un parametro supportato dal controllo, tale parametro mantiene il valore corrente. Puoi trovare i parametri supportati, i tipi di dati e i valori validi per un controllo richiamando l'API. GetSecurityControlDefinition

Per personalizzare i valori dei parametri di controllo in una politica di configurazione esistente

1. Richiama l'UpdateConfigurationPolicyAPI dall'account amministratore delegato nella regione principale.
2. Per il `Identifier` campo, fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione che desideri aggiornare.
3. Per l'`SecurityControlCustomParameters`oggetto, fornisci l'identificatore di ogni controllo che desideri personalizzare.
4. Per l'`Parameters`oggetto, fornisci il nome di ogni parametro che desideri personalizzare. Per ogni parametro che personalizzi, fornisci `CUSTOM`Value`Type`. Per`Value`, fornisci il tipo di dati del parametro e il valore personalizzato. Se la richiesta omette un parametro supportato dal controllo, tale parametro mantiene il valore corrente. Puoi trovare i parametri supportati, i tipi di dati e i valori validi per un controllo richiamando l'API. GetSecurityControlDefinition

Ad esempio, il AWS CLI comando seguente crea una nuova politica di configurazione con un valore personalizzato per il `daysToExpiration` parametro di`ACM.1`. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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}}}]}}}'
```

Personalizzazione dei parametri di controllo in un singolo account e regione

Se non utilizzi la configurazione centrale o disponi di un account autogestito, puoi personalizzare i parametri di controllo del tuo account in una sola regione alla volta.

Scegli il tuo metodo preferito e segui i passaggi per personalizzare i parametri di controllo. Le modifiche si applicano solo al tuo account nella regione corrente. Per personalizzare i parametri di controllo in regioni aggiuntive, ripeti i passaggi seguenti in ogni account e regione aggiuntivi in cui desideri personalizzare i parametri. Lo stesso controllo può utilizzare valori di parametro diversi in regioni diverse.

Security Hub CSPM console

Per personalizzare i valori dei parametri di controllo in un account e in una regione (console)

1. Aprire la console AWS Security Hub CSPM all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel pannello di navigazione, scegli Controlli. Nella tabella, scegli un controllo che supporti i parametri personalizzati per il quale desideri modificare i parametri. La colonna Parametri personalizzati indica quali controlli supportano i parametri personalizzati.
3. Nella pagina dei dettagli del controllo, scegli la scheda Parametri, quindi scegli Modifica.

4. Specifica i valori dei parametri desiderati.
5. Facoltativamente, nella sezione Motivo della modifica, seleziona un motivo per la personalizzazione dei parametri.
6. Scegli Save (Salva).

Security Hub CSPM API

Per personalizzare i valori dei parametri di controllo in un account e in una regione (API)

1. Richiama l'UpdateSecurityControlAPI.
2. Per`SecurityControlId`, fornisci l'ID del controllo che desideri personalizzare.
3. Per l'`Parameters`oggetto, fornisci il nome di ogni parametro che desideri personalizzare. Per ogni parametro che personalizzi, fornisci `CUSTOM`per `ValueType`. Per`Value`, fornisci il tipo di dati del parametro e il valore personalizzato. Se la richiesta omette un parametro supportato dal controllo, tale parametro mantiene il valore corrente. Puoi trovare i parametri supportati, i tipi di dati e i valori validi per un controllo richiamando l'API. GetSecurityControlDefinition
4. Facoltativamente, per`LastUpdateReason`, fornisci un motivo per personalizzare i parametri di controllo.

Ad esempio, il AWS CLI comando seguente definisce un valore personalizzato per il `daysToExpiration` parametro di. `ACM.1` Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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"
```

Ripristino dei valori dei parametri di controllo predefiniti

Un parametro di controllo può avere un valore predefinito definito da AWS Security Hub CSPM. Occasionalmente, Security Hub CSPM aggiorna il valore predefinito di un parametro per riflettere l'evoluzione delle best practice di sicurezza. Se non hai specificato un valore personalizzato per un

parametro di controllo, il controllo tiene traccia automaticamente di tali aggiornamenti e utilizza il nuovo valore predefinito.

È possibile tornare a utilizzare i valori dei parametri predefiniti per un controllo. Le istruzioni per la reversione dipendono dall'utilizzo o meno della configurazione centrale in Security Hub CSPM. La configurazione centrale è una funzionalità che l'amministratore delegato di Security Hub CSPM può utilizzare per configurare le funzionalità CSPM di Security Hub tra account e unità organizzative (Regioni AWS OU).

> **Note**
>
> Non tutti i parametri di controllo hanno un valore CSPM di Security Hub predefinito. In questi casi, quando `ValueType` è impostato su`DEFAULT`, non esiste un valore predefinito specifico utilizzato da Security Hub CSPM. Piuttosto, Security Hub CSPM ignora il parametro in assenza di un valore personalizzato.

Ripristino dei parametri di controllo predefiniti in più account e regioni

Se si utilizza la configurazione centrale, è possibile ripristinare i parametri di controllo per più account e unità organizzative gestiti centralmente nella regione principale e nelle regioni collegate.

Scegli il tuo metodo preferito e segui i passaggi per ripristinare i valori dei parametri predefiniti su più account e regioni utilizzando la configurazione centralizzata.

Security Hub CSPM console

Per ripristinare i valori dei parametri di controllo predefiniti in più account e regioni (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

   Accedi utilizzando le credenziali dell'account amministratore CSPM di Security Hub delegato nella regione d'origine.
2. Nel pannello di navigazione, scegli Impostazioni e configurazione.
3. Scegliere la scheda Policy.
4. Seleziona una policy, quindi scegli Modifica.
5. In Politica personalizzata, la sezione Controlli mostra un elenco di controlli per i quali hai specificato i parametri personalizzati.

6. Trova il controllo con uno o più valori di parametro da ripristinare. Quindi, scegli Rimuovi per ripristinare i valori predefiniti.
7. Nella sezione Account, verifica gli account o le unità organizzative a cui desideri applicare la policy.
8. Scegli Next (Successivo).
9. Rivedi le modifiche e verifica che siano corrette. Al termine, scegli Salva politica e applica. Nella tua regione di origine e in tutte le regioni collegate, questa azione sovrascrive le impostazioni di configurazione esistenti degli account e delle unità organizzative associate a questa politica di configurazione. Gli account e le unità organizzative possono essere associati a una politica di configurazione tramite applicazione diretta o ereditarietà da un genitore.

Security Hub CSPM API

Per ripristinare i valori predefiniti dei parametri di controllo in più account e regioni (API)

1. Richiama l'UpdateConfigurationPolicyAPI dall'account amministratore delegato nella regione principale.
2. Per il `Identifier` campo, fornisci l'Amazon Resource Name (ARN) o l'ID della policy che desideri aggiornare.
3. Per l'`SecurityControlCustomParameters`oggetto, fornisci l'identificatore di ogni controllo per il quale desideri ripristinare uno o più parametri.
4. Nell'`Parameters`oggetto, per ogni parametro da ripristinare, specificate `DEFAULT` il campo. `ValueType` Quando `ValueType` è impostato su`DEFAULT`, non è necessario fornire un valore per il `Value` campo. Se nella richiesta è incluso un valore, Security Hub CSPM lo ignora. Se la richiesta omette un parametro supportato dal controllo, tale parametro mantiene il valore corrente.

> **Warning**
>
> Se si omette un oggetto di controllo dal `SecurityControlCustomParameters` campo, Security Hub CSPM ripristina tutti i parametri personalizzati del controllo ai valori predefiniti. Un elenco completamente vuoto per `SecurityControlCustomParameters` ripristinare i parametri personalizzati di tutti i controlli ai valori predefiniti.

Ad esempio, il AWS CLI comando seguente riporta il parametro `daysToExpiration` di controllo `ACM.1` al valore predefinito nella politica di configurazione specificata. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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"}}}]}}}'
```

Ripristino dei parametri di controllo predefiniti in un singolo account e regione

Se non utilizzi la configurazione centrale o disponi di un account autogestito, puoi tornare a utilizzare i valori dei parametri predefiniti per il tuo account in una regione alla volta.

Scegli il tuo metodo preferito e segui i passaggi per ripristinare i valori dei parametri predefiniti per il tuo account in una singola regione. Per ripristinare i valori dei parametri predefiniti in altre regioni, ripeti questi passaggi in ogni regione aggiuntiva.

> **Note**
>
> Se disabiliti Security Hub CSPM, i parametri di controllo personalizzati vengono ripristinati. Se abiliti nuovamente Security Hub CSPM in futuro, tutti i controlli utilizzeranno i valori dei parametri predefiniti per l'avvio.

Security Hub CSPM console

Per ripristinare i valori dei parametri di controllo predefiniti in un account e in una regione (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel pannello di navigazione, scegli Controlli. Scegli il controllo per il quale desideri ripristinare i valori dei parametri predefiniti.
3. Nella `Parameters` scheda, scegli Personalizzato accanto a un parametro di controllo. Quindi, scegli Rimuovi personalizzazione. Questo parametro ora utilizza il valore CSPM predefinito di Security Hub e tiene traccia degli aggiornamenti futuri al valore predefinito.
4. Ripetere il passaggio precedente per ogni valore del parametro che si desidera ripristinare.

Security Hub CSPM API

Per ripristinare i valori predefiniti dei parametri di controllo in un account e in una regione (API)

1. Richiama l'API. UpdateSecurityControl
2. Per`SecurityControlId`, fornisci l'ARN o l'ID del controllo di cui desideri ripristinare i parametri.
3. Nell'`Parameters`oggetto, per ogni parametro che desideri ripristinare, fornisci `DEFAULT` il campo. `ValueType` Quando `ValueType` è impostato su`DEFAULT`, non è necessario fornire un valore per il `Value` campo. Se nella richiesta è incluso un valore, Security Hub CSPM lo ignora.
4. Facoltativamente, per`LastUpdateReason`, fornisci un motivo per tornare ai valori dei parametri predefiniti.

Ad esempio, il AWS CLI comando seguente ripristina il valore predefinito del parametro `ACM.1` di `daysToExpiration` controllo. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

Verifica dello stato delle modifiche ai parametri di controllo

Quando si tenta di personalizzare un parametro di controllo o di ripristinare il valore predefinito, è possibile verificare se le modifiche desiderate sono state effettive. Questo aiuta a garantire che un controllo funzioni come previsto e fornisce il valore di sicurezza previsto. Se l'aggiornamento di un parametro non ha esito positivo, Security Hub CSPM mantiene il valore corrente del parametro.

Per verificare che l'aggiornamento di un parametro sia andato a buon fine, è possibile esaminare i dettagli del controllo sulla console Security Hub CSPM. Sulla console, scegli Controlli nel pannello di navigazione. Quindi, scegli un controllo per visualizzarne i dettagli. La scheda Parametri mostra lo stato della modifica del parametro.

A livello di programmazione, se la richiesta di aggiornamento di un parametro è valida, il valore del `UpdateStatus` campo è `UPDATING` una risposta all'BatchGetSecurityControlsoperazione. Ciò significa che l'aggiornamento era valido, ma tutti i risultati potrebbero non includere ancora i valori dei parametri aggiornati. Quando il valore di `UpdateState` cambia in`READY`, Security Hub CSPM utilizza i valori dei parametri di controllo aggiornati durante l'esecuzione dei controlli di sicurezza del controllo. I risultati includono i valori dei parametri aggiornati.

L'`UpdateSecurityControl`operazione restituisce una `InvalidInputException` risposta per i valori dei parametri non validi. La risposta fornisce ulteriori dettagli sul motivo dell'errore. Ad esempio, potresti aver specificato un valore che non rientra nell'intervallo valido per un parametro. Oppure, potresti aver specificato un valore che non utilizza il tipo di dati corretto. Invia nuovamente la richiesta con un input valido.

Se si verifica un errore interno quando si tenta di aggiornare il valore di un parametro, Security Hub CSPM riprova automaticamente se è stato abilitato. AWS Config Per ulteriori informazioni, consulta Considerazioni prima dell'attivazione e della configurazione AWS Config.

Revisione e gestione dei risultati di controllo in Security Hub CSPM

La pagina dei dettagli del controllo mostra un elenco di risultati attivi per un controllo. L'elenco non include i risultati archiviati.

La pagina dei dettagli del controllo supporta l'aggregazione tra regioni. Se è stata impostata una regione di aggregazione, lo stato del controllo e l'elenco dei controlli di sicurezza nella pagina dei dettagli del controllo includono i controlli provenienti da tutti i collegamenti. Regioni AWS

L'elenco fornisce strumenti per filtrare e ordinare i risultati, in modo che tu possa concentrarti prima sui risultati più urgenti. Una scoperta può includere collegamenti ai dettagli delle risorse nella relativa console di servizio. Per i controlli basati su AWS Config regole, è possibile visualizzare i dettagli sulla regola.

Puoi anche utilizzare l'API CSPM AWS di Security Hub per recuperare un elenco di risultati e dettagli delle scoperte.

Per ulteriori informazioni, consulta Revisione dei dettagli e della cronologia dei risultati.

Per riflettere lo stato attuale dell'indagine su un risultato di controllo, imposti lo stato del flusso di lavoro. Per ulteriori informazioni, consulta the section called "Impostazione dello stato dei risultati del flusso di lavoro".

Puoi anche inviare alcuni risultati CSPM di Security Hub a un'azione personalizzata in Amazon. EventBridge Per ulteriori informazioni, consulta the section called "Invio dei risultati a un'operazione personalizzata".

Argomenti

- Filtraggio e ordinamento dei risultati del controllo
- Esempi di risultati di controllo

Filtraggio e ordinamento dei risultati del controllo

La selezione di un controllo dalla pagina Controlli della console AWS Security Hub CSPM o dalla pagina dei dettagli di uno standard porta alla pagina dei dettagli del controllo.

La pagina dei dettagli del controllo mostra il titolo e la descrizione del controllo, lo stato generale del controllo e un'analisi dettagliata dei controlli di sicurezza per il controllo nelle ultime 24 ore.

Utilizza le opzioni Filtra per accanto all'elenco dei controlli di controllo per concentrarti rapidamente sui risultati con uno stato del flusso di lavoro o uno stato di conformità specifici.

Oltre alle opzioni Filtra per, puoi utilizzare la casella Aggiungi filtro per filtrare l'elenco dei controlli in base ad altri campi, come Account AWS ID o ID risorsa.

Per impostazione predefinita, i risultati con uno stato di conformità PASSES vengono elencati per primi. È possibile modificare l'ordinamento predefinito scegliendo un'opzione diversa nelle intestazioni delle colonne.

Dalla pagina dei dettagli del controllo, puoi scegliere Scarica per scaricare la pagina corrente dei risultati del controllo in un file.csv.

Se filtri l'elenco dei risultati, il download include solo i controlli che corrispondono al filtro. Se si selezionano risultati specifici dall'elenco, il download include solo i risultati selezionati.

Per ulteriori informazioni sul filtraggio dei risultati, consultaFiltraggio dei risultati in Security Hub CSPM.

Esempi di risultati di controllo

Gli esempi seguenti forniscono esempi di risultati del controllo CSPM di AWS Security Hub nel AWS Security Finding Format (ASFF). Il contenuto dei risultati di controllo varia a seconda che siano stati abilitati o meno i risultati di controllo consolidati.

Se abiliti i risultati del controllo consolidato, Security Hub CSPM genera un singolo risultato per un controllo, anche se il controllo si applica a più standard abilitati. Se non abiliti questa funzionalità, Security Hub CSPM genera un risultato di controllo separato per ogni standard abilitato a cui si applica un controllo. Ad esempio, se si abilitano due standard e un controllo si applica a entrambi, si ottengono due risultati distinti per il controllo, uno per ogni standard. Se si abilitano i risultati del controllo consolidato, si riceve un solo risultato per il controllo. Per ulteriori informazioni, consulta Risultati di controllo consolidati.

Gli esempi in questa pagina forniscono esempi per entrambi gli scenari. Gli esempi includono: risultati di controllo per i singoli standard CSPM di Security Hub quando i risultati del controllo consolidato sono disabilitati e risultati di controllo per più standard CSPM di Security Hub quando i risultati del controllo consolidato sono abilitati.

Esempi di risultati del controllo

- Esempio di risultato perAWSStandard di buone pratiche di sicurezza di base
- Esempio di ricerca per il CISAWSFoundations Benchmark v5.0.0
- Esempio di ricerca per il CISAWSFoundations Benchmark v3.0.0
- Esempio di ricerca per il CISAWSFoundations Benchmark v1.4.0
- Esempio di ricerca per il CISAWSFoundations Benchmark v1.2.0
- Risultati di esempio per lo standard NIST SP 800-53 Revisione 5
- Esempio di risultato per lo standard NIST SP 800-171 Revisione 2
- Esempio di risultato relativo allo standard di sicurezza dei dati del settore delle carte di pagamento v3.2.1

- Esempio di risultato perAWSStandard di etichettatura delle risorse
- Esempio di risultato perAWS Control Towerstandard gestito dal servizio
- Esempio di risultato consolidato per più standard

> **Note**
>
> I risultati del controllo fanno riferimento a campi e valori diversi nelle regioni e nelle AWS GovCloud (US) regioni della Cina. Per ulteriori informazioni, consulta Impatto del consolidamento sui campi e sui valori ASFF.

Esempio di risultato perAWSStandard di buone pratiche di sicurezza di base

L'esempio seguente fornisce un esempio di risultato relativo a un controllo che si applica allo standard AWS Foundational Security Best Practices (FSBP). In questo esempio, i risultati del controllo consolidato sono disabilitati.

```
{
  "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"
    ]
  }
}
```

Esempio di ricerca per il CISAWSFoundations Benchmark v5.0.0

L'esempio seguente fornisce un esempio di risultato per un controllo che si applica a CIS AWS Foundations Benchmark v5.0.0. In questo esempio, i risultati del controllo consolidato sono disabilitati.

```
{
  "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"
}
```

Esempio di ricerca per il CISAWSFoundations Benchmark v3.0.0

L'esempio seguente fornisce un esempio di risultato per un controllo che si applica a CIS AWS Foundations Benchmark v3.0.0. In questo esempio, i risultati del controllo consolidato sono disabilitati.


```
{
  "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"
}
```

Esempio di ricerca per il CISAWSFoundations Benchmark v1.4.0

L'esempio seguente fornisce un esempio di risultato per un controllo che si applica a CIS AWS Foundations Benchmark v1.4.0. In questo esempio, i risultati del controllo consolidato sono disabilitati.

```
{
  "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"
    ]
  }
}
```

Esempio di ricerca per il CISAWSFoundations Benchmark v1.2.0

L'esempio seguente fornisce un esempio di risultato per un controllo che si applica a CIS AWS Foundations Benchmark v1.2.0. In questo esempio, i risultati del controllo consolidato sono disabilitati.

```
{
  "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"
    ]
  }
}
```

Risultati di esempio per lo standard NIST SP 800-53 Revisione 5

L'esempio seguente fornisce un esempio di risultato relativo a un controllo che si applica allo standard NIST SP 800-53 Revisione 5. In questo esempio, i risultati del controllo consolidato sono disabilitati.


```
{
  "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"
}
```

Esempio di risultato per lo standard NIST SP 800-171 Revisione 2

L'esempio seguente fornisce un esempio di risultato relativo a un controllo che si applica allo standard NIST SP 800-171 Revisione 2. In questo esempio, i risultati del controllo consolidato sono disabilitati.

```
{
  "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"
}
```

Esempio di risultato relativo allo standard di sicurezza dei dati del settore delle carte di pagamento v3.2.1

L'esempio seguente fornisce un esempio di risultato relativo a un controllo che si applica al Payment Card Industry Data Security Standard (PCI DSS) v3.2.1. In questo esempio, i risultati del controllo consolidato sono disabilitati.

```
{
  "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"
```

```
    ]
  }
}
```

Esempio di risultato perAWSStandard di etichettatura delle risorse

L'esempio seguente fornisce un esempio di risultato di un controllo che si applica allo standard AWS Resource Tagging. In questo esempio, i risultati del controllo consolidato sono disabilitati.

```
{
  "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"
}
```

Esempio di risultato perAWS Control Towerstandard gestito dal servizio

L'esempio seguente fornisce un esempio di risultato relativo a un controllo applicabile allo standard gestito dai AWS Control Tower servizi. In questo esempio, i risultati del controllo consolidato sono disabilitati.

```
{
  "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"
    ]
  }
}
```

Esempio di risultato consolidato per più standard

L'esempio seguente fornisce un esempio di risultato relativo a un controllo che si applica a più standard abilitati. In questo esempio, i risultati del controllo consolidato sono abilitati.

```
{
  "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"
}
```

Comprendere le integrazioni in Security Hub CSPM

AWS Security Hub CSPM può acquisire i risultati di sicurezza da diverse Servizi AWS soluzioni di sicurezza di terze parti AWS Partner Network supportate. Queste integrazioni possono aiutarti a ottenere una visione completa della sicurezza e della conformità in tutto l'ambiente. AWS Security Hub CSPM acquisisce i risultati da soluzioni integrate e li converte nel AWS Security Finding Format (ASFF).

> **Important**
>
> Per le integrazioni di prodotti supportati AWS e di terze parti, Security Hub CSPM riceve e consolida i risultati generati solo dopo aver abilitato Security Hub CSPM per il tuo. Account AWS Il servizio non riceve e consolida retroattivamente i risultati di sicurezza generati prima dell'attivazione del Security Hub CSPM.

La pagina Integrazioni della console CSPM di Security Hub fornisce l'accesso alle integrazioni di prodotti disponibili AWS e di terze parti. L'API CSPM Security Hub dispone anche di operazioni per la gestione delle integrazioni.

Un'integrazione potrebbe non essere disponibile in tutte. Regioni AWS Se un'integrazione non è supportata nella regione a cui hai attualmente effettuato l'accesso sulla console CSPM di Security Hub, non viene visualizzata nella pagina Integrazioni della console. Per un elenco delle integrazioni disponibili nelle regioni della Cina e AWS GovCloud (US) Regions, consultaDisponibilità di integrazioni per regione.

Oltre alle Servizio AWS integrazioni integrate di terze parti, puoi integrare prodotti di sicurezza personalizzati con Security Hub CSPM. È quindi possibile inviare i risultati di questi prodotti a Security Hub CSPM utilizzando l'API CSPM di Security Hub. Puoi anche utilizzare l'API per aggiornare i risultati esistenti che Security Hub CSPM ha ricevuto da un prodotto di sicurezza personalizzato.

Argomenti

- Revisione di un elenco di integrazioni CSPM di Security Hub
- Abilitazione del flusso di risultati da un'integrazione CSPM di Security Hub
- Disabilitazione del flusso di risultati da un'integrazione CSPM di Security Hub
- Visualizzazione dei risultati di un'integrazione CSPM di Security Hub
- Servizio AWS integrazioni con Security Hub CSPM
- Third-party integrazioni di prodotti con Security Hub CSPM
- Integrazione di Security Hub CSPM con prodotti personalizzati

Revisione di un elenco di integrazioni CSPM di Security Hub

Scegli il tuo metodo preferito e segui i passaggi per esaminare un elenco di integrazioni in AWS Security Hub CSPM o i dettagli su un'integrazione specifica.

Security Hub CSPM console

Per esaminare le opzioni e i dettagli di integrazione (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel pannello di navigazione CSPM di Security Hub, scegli Integrazioni.

Nella pagina Integrazioni, le integrazioni con altri Servizi AWS sono elencate per prime, seguite dalle integrazioni con prodotti di terze parti.

Per ogni integrazione, la pagina Integrazioni fornisce le seguenti informazioni:

- Il nome della società
- Il nome del prodotto
- La descrizione dell'integrazione
- Le categorie a cui l'integrazione si applica

- Come abilitare l'integrazione
- Lo stato attuale dell'integrazione

Puoi filtrare l'elenco inserendo il testo dai seguenti campi:

- Company name (Nome dell'azienda)
- Product name (Nome del prodotto)
- Integration description (Descrizione dell'integrazione)
- Categories

Security Hub CSPM API

Per esaminare le opzioni e i dettagli di integrazione (API)

Per ottenere un elenco di integrazioni, usa l'DescribeProductsoperazione. Se stai usando AWS CLI, esegui il describe-productscomando.

Per recuperare i dettagli per un'integrazione di prodotto specifica, utilizza il `ProductArn` parametro per specificare l'Amazon Resource Name (ARN) dell'integrazione.

Ad esempio, il AWS CLI comando seguente recupera i dettagli sull'integrazione CSPM di Security Hub con 3CoreSec.

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Abilitazione del flusso di risultati da un'integrazione CSPM di Security Hub

Nella pagina Integrazioni della console CSPM di AWS Security Hub, puoi vedere i passaggi necessari per abilitare ciascuna integrazione.

Per la maggior parte delle integrazioni con altri Servizi AWS, l'unico passaggio richiesto per abilitare l'integrazione è abilitare l'altro servizio. Le informazioni sull'integrazione includono un collegamento alla home page dell'altro servizio. Quando si abilita l'altro servizio, viene quindi creata e applicata automaticamente un'autorizzazione a livello di risorsa che consente a Security Hub CSPM di ricevere i risultati dal servizio.

Per le integrazioni di prodotti di terze parti, potrebbe essere necessario acquistare l'integrazione da e quindi configurare l'integrazione. Marketplace AWS Le informazioni sull'integrazione forniscono collegamenti per completare queste attività.

Se è disponibile più di una versione di un prodotto Marketplace AWS, seleziona la versione a cui desideri abbonarti, quindi scegli Continua con la sottoscrizione. Ad esempio, alcuni prodotti offrono una versione standard e una AWS GovCloud (US) versione.

Quando abiliti un'integrazione di prodotto, una policy delle risorse viene automaticamente collegata a tale sottoscrizione prodotto. Questa politica delle risorse definisce le autorizzazioni di cui Security Hub CSPM ha bisogno per ricevere i risultati da quel prodotto.

Dopo aver completato i passaggi preliminari per abilitare un'integrazione, puoi disabilitare e riattivare il flusso di risultati di tale integrazione. Nella pagina Integrazioni, per le integrazioni che inviano risultati, le informazioni sullo stato indicano se i risultati sono attualmente accettati.

Security Hub CSPM console

Per abilitare il flusso dei risultati da un'integrazione (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel pannello di navigazione CSPM di Security Hub, scegli Integrazioni.
3. Per le integrazioni che inviano risultati, le informazioni sullo stato indicano se Security Hub CSPM sta attualmente accettando i risultati di tale integrazione.
4. Scegli Accetta i risultati.

Security Hub CSPM API

Usa l'EnableImportFindingsForProductoperazione. Se stai usando AWS CLI, esegui il enable-import-findings-for-productcomando. Per consentire a Security Hub di ricevere i risultati di un'integrazione, è necessario l'ARN del prodotto. Per ottenere gli ARN per le integrazioni disponibili, utilizza l'operazione. DescribeProducts Se utilizzi il AWS CLI, esegui il. describe-products

Ad esempio, il AWS CLI comando seguente consente a Security Hub CSPM di ricevere i risultati dall'integrazione CrowdStrike Falcon. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Disabilitazione del flusso di risultati da un'integrazione CSPM di Security Hub

Scegli il tuo metodo preferito e segui i passaggi per disabilitare il flusso di risultati da un'integrazione CSPM AWS di Security Hub.

Security Hub CSPM console

Per disabilitare il flusso di risultati da un'integrazione (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel pannello di navigazione CSPM di Security Hub, scegli Integrazioni.
3. Per le integrazioni che inviano risultati, le informazioni sullo stato indicano se Security Hub CSPM sta attualmente accettando i risultati di tale integrazione.
4. Scegli Smetti di accettare i risultati.

Security Hub CSPM API

Usa l'DisableImportFindingsForProductoperazione. Se stai usando AWS CLI, esegui il disable-import-findings-for-productcomando. Per disabilitare il flusso di risultati da un'integrazione, è necessario l'ARN dell'abbonamento per l'integrazione abilitata. Per ottenere l'ARN dell'abbonamento, utilizzare l'ListEnabledProductsForImportoperazione. Se stai usando il AWS CLI, esegui il list-enabled-products-for-import.

Ad esempio, il AWS CLI comando seguente disabilita il flusso di risultati verso Security Hub CSPM dall' CrowdStrike integrazione Falcon. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

Visualizzazione dei risultati di un'integrazione CSPM di Security Hub

Quando inizi ad accettare i risultati da un'integrazione CSPM di AWS Security Hub, la pagina Integrazioni della console CSPM di Security Hub mostra lo stato dell'integrazione come Accettazione dei risultati. Per esaminare un elenco dei risultati dell'integrazione, scegli Vedi risultati.

L'elenco dei risultati mostra i risultati attivi per l'integrazione selezionata che hanno lo stato del flusso di lavoro `NEW` o `NOTIFIED`.

Se abiliti l'aggregazione tra regioni, nella regione di aggregazione l'elenco include i risultati della regione di aggregazione e delle regioni collegate in cui è abilitata l'integrazione. Security Hub non abilita automaticamente le integrazioni basate sulla configurazione di aggregazione interregionale.

In altre regioni, l'elenco dei risultati di un'integrazione contiene solo i risultati della regione corrente.

Per informazioni su come configurare l'aggregazione tra regioni, vedere. the section called "Aggregazione dei dati tra le regioni"

Dall'elenco dei risultati puoi eseguire le seguenti operazioni.

- Modificare filtri e raggruppamento dell'elenco
- Visualizzare i dettagli per i singoli risultati
- Aggiornare lo stato del flusso di lavoro dei risultati
- Inviare i risultati alle operazioni personalizzate

Servizio AWS integrazioni con Security Hub CSPM

AWS Security Hub CSPM supporta integrazioni con molti altri. Servizi AWS Queste integrazioni possono aiutarti a ottenere una visione completa della sicurezza e della conformità in tutto il tuo ambiente. AWS

Salvo diversa indicazione di seguito, Servizio AWS le integrazioni che inviano i risultati a Security Hub CSPM vengono attivate automaticamente dopo aver abilitato Security Hub CSPM e l'altro servizio. Le integrazioni che ricevono i risultati CSPM di Security Hub potrebbero richiedere passaggi aggiuntivi per l'attivazione. Consulta le informazioni su ciascuna integrazione per saperne di più.

Alcune integrazioni non sono disponibili in tutte Regioni AWS. Nella console Security Hub CSPM, un'integrazione non viene visualizzata nella pagina Integrazioni se non è supportata nella regione

corrente. Per un elenco delle integrazioni disponibili nelle regioni della Cina e AWS GovCloud (US) Regions, consultaDisponibilità di integrazioni per regione.

Panoramica di AWS integrazioni di servizi con Security Hub CSPM

La tabella seguente fornisce una panoramica dei AWS servizi che inviano risultati a Security Hub CSPM o ricevono risultati da Security Hub CSPM.

Servizio integrato AWS	Direzione
AWS Config	Invia i risultati
AWS Firewall Manager	Invia i risultati
Amazon GuardDuty	Invia i risultati
AWS Health	Invia i risultati
AWS Identity and Access Management Access Analyzer	Invia i risultati
Amazon Inspector	Invia i risultati
AWS IoT Device Defender	Invia i risultati
Amazon Macie	Invia i risultati
Amazon Route 53 Resolver Firewall DNS	Invia i risultati
AWS Systems Manager Gestione patch	Invia i risultati
AWS Audit Manager	Riceve i risultati
Amazon Q Developer nelle applicazioni di chat	Riceve i risultati
Amazon Detective	Riceve i risultati
Amazon Security Lake	Riceve i risultati

Servizio integrato AWS	Direzione	
AWS Systems Manager Explorer e OpsCenter	Riceve e aggiorna i risultati	
AWS Trusted Advisor	Riceve i risultati	

Servizi AWS che inviano i risultati al Security Hub CSPM

Quanto segue si Servizi AWS integra e può inviare i risultati al Security Hub CSPM. Security Hub CSPM converte i risultati nel formato AWS Security Finding.

AWS Config (Invia i risultati)

AWS Config è un servizio che consente di valutare, controllare e valutare le configurazioni delle AWS risorse. AWS Config monitora e registra continuamente le configurazioni AWS delle risorse e consente di automatizzare la valutazione delle configurazioni registrate rispetto alle configurazioni desiderate.

Utilizzando l'integrazione con AWS Config, è possibile visualizzare i risultati delle valutazioni delle regole AWS Config gestite e personalizzate come risultati in Security Hub CSPM. Questi risultati possono essere visualizzati insieme ad altri risultati CSPM di Security Hub, fornendo una panoramica completa del livello di sicurezza.

AWS Config utilizza Amazon EventBridge per inviare valutazioni delle AWS Config regole a Security Hub CSPM. Security Hub CSPM trasforma le valutazioni delle regole in risultati che seguono il AWS Security Finding Format. Security Hub CSPM arricchisce quindi i risultati nel miglior modo possibile ottenendo ulteriori informazioni sulle risorse interessate, come Amazon Resource Name (ARN), i tag delle risorse e la data di creazione.

Per ulteriori informazioni su questa integrazione, consulta le seguenti sezioni.

In che modo AWS Config invia i risultati al Security Hub CSPM

Tutti i risultati in Security Hub CSPM utilizzano il formato JSON standard di ASFF. ASFF include dettagli sull'origine del risultato, sulla risorsa interessata e sullo stato attuale del risultato. AWS Config invia valutazioni di regole gestite e personalizzate a Security Hub CSPM tramite. EventBridge Security Hub CSPM trasforma le valutazioni delle regole in risultati che seguono ASFF e arricchisce i risultati con il massimo impegno.

Tipi di risultati che AWS Config invia a Security Hub CSPM

Dopo l'attivazione dell'integrazione, AWS Config invia le valutazioni di tutte le regole AWS Config gestite e le regole personalizzate a Security Hub CSPM. Vengono inviate solo le valutazioni eseguite dopo l'attivazione del CSPM di Security Hub. Ad esempio, supponiamo che la valutazione di una AWS Config regola riveli cinque risorse fallite. Se abiliti Security Hub CSPM dopo quella valutazione e la regola rivela una sesta risorsa fallita, AWS Config invia solo la valutazione della sesta risorsa a Security Hub CSPM.

Sono escluse le valutazioni AWS Config delle regole collegate ai servizi, come quelle utilizzate per eseguire i controlli CSPM di Security Hub. L'eccezione sono i risultati generati da regole collegate ai servizi che creano e gestiscono. AWS Control Tower AWS Config L'inclusione dei risultati di queste regole aiuta a garantire che i dati dei risultati includano i risultati dei controlli proattivi eseguiti da. AWS Control Tower

Invio AWS Config risultati del Security Hub CSPM

Quando l'integrazione è attivata, Security Hub CSPM assegnerà automaticamente le autorizzazioni necessarie per ricevere i risultati da. AWS Config Security Hub CSPM utilizza autorizzazioni a livello di servizio che forniscono un modo sicuro per attivare questa integrazione e importare i risultati da Amazon. AWS Config EventBridge

Latenza per l'invio degli esiti

Quando si AWS Config crea un nuovo risultato, in genere è possibile visualizzarlo in Security Hub CSPM entro cinque minuti.

Riprovare quando Security Hub CSPM non è disponibile

AWS Config invia i risultati al Security Hub CSPM con la massima diligenza possibile tramite. EventBridge Quando un evento non viene consegnato correttamente a Security Hub CSPM, EventBridge riprova la consegna per un massimo di 24 ore o 185 volte, a seconda dell'evento che si verifica per primo.

Aggiornamento esistente AWS Config risultati in Security Hub CSPM

Dopo aver AWS Config inviato un risultato a Security Hub CSPM, può inviare aggiornamenti dello stesso risultato a Security Hub CSPM per riflettere ulteriori osservazioni sull'attività di ricerca. Gli aggiornamenti vengono inviati solo per gli eventi. `ComplianceChangeNotification` Se non si verifica alcuna modifica della conformità, gli aggiornamenti non vengono inviati al Security Hub

CSPM. Security Hub CSPM elimina i risultati 90 giorni dopo l'aggiornamento più recente o 90 giorni dopo la creazione se non si verifica alcun aggiornamento.

Security Hub CSPM non archivia i risultati da cui vengono inviati AWS Config anche se si elimina la risorsa associata.

Regioni in cui AWS Config esistono risultati

AWS Config i risultati avvengono su base regionale. AWS Config invia i risultati al Security Hub CSPM nella stessa regione o nelle stesse regioni in cui si verificano i risultati.

Visualizzazione AWS Config risultati in Security Hub CSPM

Per visualizzare i AWS Config risultati, scegli Findings dal riquadro di navigazione CSPM di Security Hub. Per filtrare i risultati in modo da visualizzare solo AWS Config i risultati, scegli Nome prodotto nel menu a discesa della barra di ricerca. Immettete Config e scegliete Applica.

Interpretazione AWS Config ricerca di nomi in Security Hub CSPM

Security Hub CSPM trasforma le valutazioni delle AWS Config regole in risultati che seguono il. AWS Formato ASFF (Security Finding Format) AWS Config le valutazioni delle regole utilizzano un pattern di eventi diverso rispetto a ASFF. La tabella seguente mappa i campi di valutazione delle AWS Config regole con la loro controparte ASFF così come appaiono in Security Hub CSPM.

Tipo di risultato per la valutazione delle regole di Config	Tipo di risultati ASFF	Valore codificato
detail.aws AccountId	AwsAccountId	
dettaglio.nuovo Evaluatio nResult.resultRecordedTime	CreatedAt	
dettaglio.nuovo Evaluatio nResult.resultRecordedTime	UpdatedAt	
	ProductArn	<partition><region>«arn:: securityhub:: /config» product/ aws
	ProductName	«Config»

Tipo di risultato per la valutazione delle regole di Config	Tipo di risultati ASFF	Valore codificato
	CompanyName	"AWS"
	Region	«eu-central-1"
configurazione RuleArn	GeneratorId, ProductFields	
dettaglio. ConfigRuleARN/finding/hash	Id	
dettaglio.config RuleName	Titolo, ProductFields	
detail.config RuleName	Description	«Questo risultato è stato creato per una modifica della conformità delle risorse per la regola di configurazione:» `${detail.ConfigRuleName}`
Elemento di configurazione «ARN» o ARN calcolato da CSPM di Security Hub	Risorse [i] .id	
Detail.ResourceType	Risorse [i] .Type	"AwsS3Bucket"
	Risorse [i] .Partizione	"aws"
	Risorse [i] .Region	«eu-central-1"
Elemento di configurazione «configuration»	Risorse [i] .Dettagli	
	SchemaVersion	«2018-10-08"
	Severity.Label	Vedi «Interpretazione dell'etichetta di severità» di seguito

Tipo di risultato per la valutazione delle regole di Config	Tipo di risultati ASFF	Valore codificato
	Tipi	["Controlli del software e della configurazione"]
dettaglio.nuovo EvaluationResult.complianceType	Compliance.Status	«FAILED», «NOT_AVAILABLE», «PASSED» o «WARNING»
	Workflow.Status	«RISOLTO» se un AWS Config risultato viene generato con un valore « Compliance.Status PASSED» o se il risultato Compliance.Status passa da «FAILED» a «PASSED». Altrimenti, Workflow.Status sarà «NUOVO». È possibile modificare questo valore con l'operazione BatchUpdateFindingsAPI.

Interpretazione dell'etichetta di gravità

Tutti i risultati delle valutazioni delle AWS Config regole hanno un'etichetta di gravità predefinita pari a MEDIUM nell'ASFF. È possibile aggiornare l'etichetta di gravità di un risultato con l'operazione `BatchUpdateFindings`API.

Risultato tipico di AWS Config

Security Hub CSPM trasforma le valutazioni delle AWS Config regole in risultati che seguono l'ASFF. Di seguito è riportato un esempio di un risultato tipico dell'ASFF. AWS Config

> **Note**
>
> Se la descrizione supera i 1.024 caratteri, verrà troncata a 1.024 caratteri e alla fine verrà visualizzato «(troncato)».


```
{
 "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"
  ]
 }
}
```

Abilitazione e configurazione dell'integrazione

Dopo aver abilitato Security Hub CSPM, questa integrazione viene attivata automaticamente. AWS Config inizia immediatamente a inviare i risultati al Security Hub CSPM.

Interruzione della pubblicazione dei risultati su Security Hub CSPM

Per interrompere l'invio dei risultati a Security Hub CSPM, puoi utilizzare la console CSPM di Security Hub o l'API CSPM di Security Hub.

Per istruzioni su come interrompere il flusso dei risultati, vedere. Abilitazione del flusso di risultati da un'integrazione CSPM di Security Hub

AWS Firewall Manager (Invia i risultati)

Firewall Manager invia i risultati a Security Hub CSPM quando una politica WAF (Web Application Firewall) per le risorse o una regola della lista di controllo degli accessi Web (Web Access Control List) non è conforme. Firewall Manager invia i risultati anche quando AWS Shield Advanced non protegge le risorse o quando viene identificato un attacco.

Dopo aver abilitato Security Hub CSPM, questa integrazione viene attivata automaticamente. Firewall Manager inizia immediatamente a inviare i risultati al Security Hub CSPM.

Per ulteriori informazioni sull'integrazione, visualizza la pagina Integrazioni nella console Security Hub CSPM.

Per ulteriori informazioni su Firewall Manager, consulta la Guida per AWS WAF gli sviluppatori.

Amazon GuardDuty (invia i risultati)

GuardDuty invia tutti i tipi di risultati che genera a Security Hub CSPM. Alcuni tipi di ricerca hanno prerequisiti, requisiti di abilitazione o limitazioni regionali. Per ulteriori informazioni, consulta la sezione GuardDuty Ricerca dei tipi nella Amazon GuardDuty User Guide.

I nuovi risultati GuardDuty vengono inviati al Security Hub CSPM entro cinque minuti. Gli aggiornamenti ai risultati vengono inviati in base all'impostazione Updated found per Amazon EventBridge nelle GuardDuty impostazioni.

Quando si generano risultati di GuardDuty esempio utilizzando la pagina GuardDuty Impostazioni, Security Hub CSPM riceve i risultati del campione e omette il prefisso `[Sample]` nel tipo di risultato. Ad esempio, il tipo di ricerca del campione in GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions` viene visualizzato come `Recon:IAMUser/ResourcePermissions` in Security Hub CSPM.

Dopo aver abilitato Security Hub CSPM, questa integrazione viene attivata automaticamente. GuardDutyinizia immediatamente a inviare i risultati al Security Hub CSPM.

Per ulteriori informazioni sull' GuardDuty integrazione, consulta Integrating with AWS Security Hub CSPM nella Amazon GuardDuty User Guide.

AWS Health (Invia i risultati)

AWS Health offre una visibilità continua sulle prestazioni delle risorse e sulla disponibilità delle tue Servizi AWS e Account AWS. È possibile utilizzare AWS Health gli eventi per scoprire in che modo le modifiche ai servizi e alle risorse potrebbero influire sulle applicazioni su cui vengono eseguite AWS.

L'integrazione con AWS Health non utilizza`BatchImportFindings`. AWS Health Utilizza invece la messaggistica di eventi da servizio a servizio per inviare i risultati a Security Hub CSPM.

Per ulteriori informazioni sull'integrazione, consulta le seguenti sezioni.

In che modo AWS Health invia i risultati al Security Hub CSPM

In CSPM Security Hub, i problemi di sicurezza vengono monitorati come esiti. Alcuni risultati derivano da problemi rilevati da altri AWS servizi o da partner terzi. Security Hub CSPM dispone anche di una serie di regole che utilizza per rilevare problemi di sicurezza e generare risultati.

CSPM Security Hub fornisce strumenti per gestire gli esiti da tutte queste origini. È possibile visualizzare e filtrare gli elenchi di esiti e visualizzare i dettagli per un riscontro. Consulta Revisione dei dettagli e della cronologia dei risultati in Security Hub CSPM. È inoltre possibile monitorare lo stato di un'indagine in un esito. Consulta Impostazione dello stato del flusso di lavoro dei risultati in Security Hub CSPM.

Tutti i risultati in Security Hub CSPM utilizzano un formato JSON standard chiamato. AWS Formato ASFF (Security Finding Format) ASFF include dettagli sull'origine del problema, sulle risorse interessate e sullo stato attuale del risultato.

AWS Health è uno dei AWS servizi che invia i risultati al Security Hub CSPM.

Tipi di risultati che AWS Health invia a Security Hub CSPM

Dopo aver abilitato l'integrazione, AWS Health invia i risultati che soddisfano una o più delle specifiche elencate a Security Hub CSPM. Security Hub CSPM inserisce i risultati in. AWS Formato ASFF (Security Finding Format)

- Risultati che contengono uno dei seguenti valori per: Servizio AWS
  - `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

- ~~Risultati con `security` le `abuse` parole o `certificate` sul AWS Health `typeCode` campo~~
- Risultati in cui si trova il AWS Health servizio `risk` o `abuse`

Invio AWS Health risultati del Security Hub CSPM

Quando scegli di accettare i risultati da AWS Health, Security Hub CSPM assegnerà automaticamente le autorizzazioni necessarie per ricevere i risultati. AWS Health Security Hub CSPM utilizza autorizzazioni a livello di servizio che ti offrono un modo semplice e sicuro per abilitare questa integrazione e importare i risultati da Amazon per tuo conto. AWS Health EventBridge Scegliendo Accept Findings si concede a Security Hub l'autorizzazione CSPM di utilizzare i risultati da. AWS Health

Latenza per l'invio degli esiti

Quando viene AWS Health creato un nuovo risultato, di solito viene inviato a Security Hub CSPM entro cinque minuti.

Riprovare quando Security Hub CSPM non è disponibile

AWS Health invia i risultati al Security Hub CSPM con la massima diligenza possibile tramite. EventBridge Quando un evento non viene inviato correttamente a Security Hub CSPM, EventBridge riprova a inviarlo per 24 ore.

Aggiornamento degli esiti esistenti CSPM Security Hub

Dopo aver AWS Health inviato un risultato a Security Hub CSPM, può inviare aggiornamenti allo stesso risultato per riflettere ulteriori osservazioni sull'attività di ricerca a Security Hub CSPM.

Regioni in cui esistono i risultati

Per gli eventi globali, AWS Health invia i risultati al Security Hub CSPM in us-east-1 (AWS partizione), cn-northwest-1 (partizione per la Cina) e gov-us-west-1 (partizione). GovCloud AWS Health invia Region-specific eventi a Security Hub CSPM nella stessa regione o nelle stesse regioni in cui si verificano gli eventi.

Visualizzazione AWS Health risultati in Security Hub CSPM

Per visualizzare i AWS Health risultati in Security Hub CSPM, scegli Findings dal pannello di navigazione. Per filtrare i risultati in modo da visualizzare solo AWS Health i risultati, scegli Health dal campo Nome prodotto.

Interpretazione AWS Health ricerca di nomi in Security Hub CSPM

AWS Health invia i risultati a Security Hub CSPM utilizzando. AWS Formato ASFF (Security Finding Format) AWS Health la ricerca utilizza un pattern di eventi diverso rispetto al formato ASFF CSPM di

Security Hub. La tabella seguente descrive in dettaglio tutti i campi di AWS Health ricerca con la loro controparte ASFF così come appaiono in Security Hub CSPM.

Tipo di reperto sanitario	Tipo di risultati ASFF	Valore codificato
account	AwsAccountId	
Dettaglio. Ora di inizio	CreatedAt	
dettaglio.evento Descripti on.latestDescription	Description	
dettaglio.evento TypeCode	GeneratorId	
detail.eventArn (incluso l'account) + hash di detail.st artTime	Id	
«<region>product/awsarn:aws :securityhub::: /health»	ProductArn	
account o resourceID	Risorse [i] .id	
	Risorse [i] .Tipo	«Altro»
	SchemaVersion	«2018-10-08"
	Severity.Label	Vedi «Interpretazione dell'etic hetta di severità» di seguito
«AWS Health -» detail.event TypeCode	Titolo	
-	Tipi	["Controlli del software e della configurazione"]
event.time	UpdatedAt	
URL dell'evento sulla console Health	SourceUrl	

Interpretazione dell'etichetta di gravità

L'etichetta di gravità nel risultato ASFF viene determinata utilizzando la seguente logica:

- Severità CRITICA se:
  - Il `service` campo del AWS Health risultato ha il valore `Risk`
  - Il `typeCode` campo del AWS Health risultato ha il valore `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - Il `typeCode` campo del AWS Health risultato ha il valore `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - Il `typeCode` campo del AWS Health risultato ha il valore `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

  Severità ALTA se:
  - Il `service` campo del AWS Health risultato ha il valore `Abuse`
  - Il `typeCode` campo del AWS Health risultato contiene il valore `SECURITY_NOTIFICATION`
  - Il `typeCode` campo del AWS Health risultato contiene il valore `ABUSE_DETECTION`

  Severità MEDIUM se:
  - Il `service` campo del risultato è uno dei seguenti:`ACM`,`ARTIFACT`,`AUDITMANAGER`,`BACKUP`,`CLOUDENDURE`,`CLOUDHSM`,`CLOUDTRAIL`, `CLOUDWATCHCODEGURGU`,`COGNITO`,`CONFIG`,`CONTROLTOWER`,`DETECTIVE`,`DIRECTORYSERVICE`, `DRSEVENTS`,`FIREWALLMANAGER`,`GUARDDUTY`,`IAM`,`INSPECTOR`,`INSPECTOR2`,`IOTDEVICEDEFENDER`, `KMSMACIE`,`NETWORKFIREWALL`,`ORGANIZATIONS`,`RESILIENCEHUB`,`RESOURCEMANAGER`,`ROUTE53`,`SEC` `SECRETSMANAGERSES`,`SHIELD`,`SSO`,, `WAF`
  - Il campo TypeCode del AWS Health risultato contiene il valore `CERTIFICATE`
  - Il campo TypeCode del AWS Health risultato contiene il valore `END_OF_SUPPORT`

Risultato tipico di AWS Health

AWS Health invia i risultati a Security Hub CSPM utilizzando. AWS Formato ASFF (Security Finding Format) Di seguito è riportato un esempio di un risultato tipico di. AWS Health

> **Note**
>
> Se la descrizione supera i 1024 caratteri, verrà troncata a 1024 caratteri e alla fine verrà riportata la dicitura (troncata).


```
{
            "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"
                ]
            }
        }
    ]
}
```

Abilitazione e configurazione dell'integrazione

Dopo aver abilitato Security Hub CSPM, questa integrazione viene attivata automaticamente. AWS Health inizia immediatamente a inviare i risultati al Security Hub CSPM.

Interruzione della pubblicazione dei risultati su Security Hub CSPM

Per interrompere l'invio dei risultati a Security Hub CSPM, puoi utilizzare la console CSPM di Security Hub o l'API CSPM di Security Hub.

Per istruzioni su come interrompere il flusso dei risultati, vedere. Abilitazione del flusso di risultati da un'integrazione CSPM di Security Hub

AWS Identity and Access Management Access Analyzer (Invia i risultati)

Con IAM Access Analyzer, tutti i risultati vengono inviati a Security Hub CSPM.

IAM Access Analyzer utilizza il ragionamento basato sulla logica per analizzare le policy basate sulle risorse applicate alle risorse supportate nell'account. IAM Access Analyzer genera un risultato quando rileva una dichiarazione di policy che consente a un principale esterno di accedere a una risorsa del tuo account.

In IAM Access Analyzer, solo l'account amministratore può visualizzare i risultati degli analizzatori che si applicano a un'organizzazione. Per gli analizzatori di organizzazioni, il campo `AwsAccountId` ASFF riflette l'ID dell'account amministratore. Sotto`ProductFields`, il `ResourceOwnerAccount` campo indica l'account in cui è stato scoperto il risultato. Se abiliti gli analizzatori singolarmente per ogni account, Security Hub CSPM genera più risultati, uno che identifica l'ID dell'account amministratore e uno che identifica l'ID dell'account della risorsa.

Per ulteriori informazioni, consulta Integration with AWS Security Hub CSPM nella IAM User Guide.

Amazon Inspector (invia i risultati)

Amazon Inspector è un servizio di gestione delle vulnerabilità che analizza continuamente i carichi di lavoro alla ricerca AWS di eventuali vulnerabilità. Amazon Inspector rileva e analizza automaticamente le istanze e le immagini dei container di Amazon EC2 che si trovano nell'Amazon Elastic Container Registry. La scansione cerca le vulnerabilità del software e l'esposizione involontaria della rete.

Dopo aver abilitato Security Hub CSPM, questa integrazione viene attivata automaticamente. Amazon Inspector inizia immediatamente a inviare tutti i risultati generati a Security Hub CSPM.

Per ulteriori informazioni sull'integrazione, consulta Integration with AWS Security Hub CSPM nella Amazon Inspector User Guide.

Security Hub CSPM può anche ricevere risultati da Amazon Inspector Classic. Amazon Inspector Classic invia i risultati al CSPM di Security Hub generati tramite esecuzioni di valutazione per tutti i pacchetti di regole supportati.

Per ulteriori informazioni sull'integrazione, consulta Integration with AWS Security Hub CSPM nella Amazon Inspector Classic User Guide.

I risultati di Amazon Inspector e Amazon Inspector Classic utilizzano lo stesso ARN del prodotto. I risultati di Amazon Inspector riportano la seguente voce: `ProductFields`

```
"aws/inspector/ProductVersion": "2",
```

> **Note**
>
> I risultati di sicurezza generati da Amazon Inspector Code Security non sono disponibili per questa integrazione. Tuttavia, puoi accedere a questi risultati particolari nella console Amazon Inspector e tramite l'API Amazon Inspector.

AWS IoT Device Defender (Invia i risultati)

AWS IoT Device Defender è un servizio di sicurezza che verifica la configurazione dei dispositivi IoT, monitora i dispositivi connessi per rilevare comportamenti anomali e aiuta a mitigare i rischi per la sicurezza.

Dopo aver abilitato entrambi AWS IoT Device Defender e Security Hub CSPM, visita la pagina Integrazioni della console CSPM di Security Hub e scegli Accetta risultati per Audit, Detect o entrambi. AWS IoT Device Defender Audit and Detect inizia a inviare tutti i risultati al Security Hub CSPM.

AWS IoT Device Defender Audit invia i riepiloghi dei controlli a Security Hub CSPM, che contengono informazioni generali per un tipo di controllo e un'attività di controllo specifici. AWS IoT Device Defender Detect invia i risultati delle violazioni per l'apprendimento automatico (ML), i comportamenti statici e statici al Security Hub CSPM. Audit invia anche gli aggiornamenti dei risultati a Security Hub CSPM.

Per ulteriori informazioni su questa integrazione, consulta Integration with AWS Security Hub CSPM nella AWS IoT Developer Guide.

Amazon Macie (invia risultati)

Amazon Macie è un servizio di sicurezza dei dati che rileva dati sensibili utilizzando machine learning e la corrispondenza del modello, fornisce visibilità sui rischi legati alla sicurezza dei dati e consente una protezione automatizzata da tali rischi. Una scoperta di Macie può indicare l'esistenza di una potenziale violazione delle policy o di dati sensibili nel tuo patrimonio di dati Amazon S3.

Dopo aver abilitato Security Hub CSPM, Macie inizia automaticamente a inviare i risultati delle policy a Security Hub CSPM. Puoi configurare l'integrazione per inviare anche i risultati dei dati sensibili a Security Hub CSPM.

In Security Hub CSPM, il tipo di ricerca per una policy o una ricerca di dati sensibili viene modificato in un valore compatibile con ASFF. Ad esempio, il tipo di `Policy:IAMUser/S3BucketPublic`

ricerca in Macie viene visualizzato come `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic` in Security Hub CSPM.

Macie invia anche i risultati dei campioni generati al Security Hub CSPM. Per i risultati di esempio, il nome della risorsa interessata è `macie-sample-finding-bucket` e il valore del campo è. `Sample true`

Per ulteriori informazioni, consulta la sezione Valutazione dei risultati di Macie con Security Hub nella Guida per l'utente di Amazon Macie.

Amazon Route 53 Resolver Firewall DNS (invia i risultati)

Con Amazon Route 53 Resolver DNS Firewall, puoi filtrare e regolare il traffico DNS in uscita per il tuo cloud privato virtuale (VPC). Puoi farlo creando raccolte riutilizzabili di regole di filtraggio nei gruppi di regole del firewall DNS, associando i gruppi di regole al tuo VPC e quindi monitorando l'attività nei log e nelle metriche del firewall DNS. In base all'attività, puoi modificare il comportamento del firewall DNS. DNS Firewall è una funzionalità di Route 53 Resolver.

Route 53 Resolver DNS Firewall può inviare diversi tipi di risultati al Security Hub CSPM:

- Risultati relativi alle query bloccate o inviate avvisi per i domini associati agli elenchi di domini AWS gestiti, che sono elenchi di domini che gestisce. AWS
- Risultati relativi alle query bloccate o inviate avvisi per i domini associati a un elenco di domini personalizzato definito dall'utente.
- Risultati relativi alle query bloccate o segnalate da DNS Firewall Advanced, una funzionalità di Route 53 Resolver in grado di rilevare le query associate a minacce DNS avanzate come Domain Generation Algorithms (DGA) e DNS Tunneling.

Dopo aver abilitato Security Hub CSPM e Route 53 Resolver DNS Firewall, DNS Firewall inizia automaticamente a inviare i risultati per AWS Managed Domain Lists e DNS Firewall Advanced a Security Hub CSPM. Per inviare anche i risultati per un elenco di domini personalizzato a Security Hub CSPM, abilita manualmente l'integrazione in Security Hub CSPM.

In Security Hub CSPM, tutti i risultati di Route 53 Resolver DNS Firewall hanno il seguente tipo:. `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Per ulteriori informazioni, consulta Invio dei risultati da Route 53 Resolver DNS Firewall a Security Hub nella Amazon Route 53 Developer Guide.

AWS Systems Manager Patch Manager (invia i risultati)

AWS Systems Manager Patch Manager invia i risultati a Security Hub CSPM quando le istanze della flotta di un cliente non sono conformi allo standard di conformità delle patch.

Patch Manager automatizza il processo di applicazione di patch alle istanze gestite con aggiornamenti correlati alla sicurezza e di altro tipo.

Dopo aver abilitato Security Hub CSPM, questa integrazione viene attivata automaticamente. Systems Manager Patch Manager inizia immediatamente a inviare i risultati al Security Hub CSPM.

Per ulteriori informazioni sull'utilizzo di Patch Manager, vedere AWS Systems Manager Patch Manager nella Guida per l'AWS Systems Manager utente.

AWS servizi che ricevono risultati da Security Hub CSPM

I seguenti AWS servizi sono integrati con Security Hub CSPM e ricevono i risultati da Security Hub CSPM. Dove indicato, il servizio integrato può anche aggiornare i risultati. In questo caso, la ricerca degli aggiornamenti apportati nel servizio integrato si rifletterà anche in Security Hub CSPM.

AWS Audit Manager (Riceve i risultati)

AWS Audit Manager riceve i risultati dal Security Hub CSPM. Questi risultati aiutano gli utenti di Audit Manager a prepararsi per gli audit.

Per ulteriori informazioni su Audit Manager, consulta la Guida per l'utente di AWS Audit Manager.AWS I controlli CSPM di Security Hub supportati da AWS Audit Manager elencano i controlli per i quali Security Hub CSPM invia i risultati all'Audit Manager.

Amazon Q Developer nelle applicazioni di chat (riceve i risultati)

Amazon Q Developer nelle applicazioni di chat è un agente interattivo che ti aiuta a monitorare e interagire con AWS le tue risorse nei canali Slack e nelle chat room di Amazon Chime.

Amazon Q Developer nelle applicazioni di chat riceve i risultati dal Security Hub CSPM.

Per ulteriori informazioni sull'integrazione di Amazon Q Developer nelle applicazioni di chat con Security Hub CSPM, consulta la panoramica sull'integrazione CSPM di Security Hub nella Amazon Q Developer in chat application Administrator Guide.

Amazon Detective (riceve i risultati)

Detective raccoglie automaticamente i dati di registro dalle tue AWS risorse e utilizza l'apprendimento automatico, l'analisi statistica e la teoria dei grafi per aiutarti a visualizzare e condurre indagini di sicurezza più rapide ed efficienti.

L'integrazione CSPM di Security Hub con Detective ti consente di passare dai risultati di GuardDuty Amazon in Security Hub CSPM a Detective. Puoi quindi utilizzare gli strumenti e le visualizzazioni del Detective per indagare su di essi. L'integrazione non richiede alcuna configurazione aggiuntiva in Security Hub CSPM o Detective.

Per i risultati ricevuti da altri Servizi AWS, il pannello dei dettagli dei risultati sulla console CSPM di Security Hub include una sottosezione Investigate in Detective. Quella sottosezione contiene un collegamento a Detective dove puoi approfondire il problema di sicurezza segnalato dalla scoperta. Puoi anche creare un grafico comportamentale in Detective basato sui risultati del CSPM di Security Hub per condurre indagini più efficaci. Per ulteriori informazioni, consulta i risultati AWS di sicurezza nell'Amazon Detective Administration Guide.

Se l'aggregazione tra regioni è abilitata, quando si esegue il pivot dalla regione di aggregazione, Detective si apre nella regione in cui ha avuto origine il risultato.

Se un collegamento non funziona, per consigli sulla risoluzione dei problemi, consulta la sezione relativa alla risoluzione dei problemi del pivot.

Amazon Security Lake (riceve i risultati)

Security Lake è un servizio di data lake di sicurezza completamente gestito. Puoi utilizzare Security Lake per centralizzare automaticamente i dati di sicurezza provenienti da fonti cloud, locali e personalizzate in un data lake archiviato nel tuo account. Gli abbonati possono utilizzare i dati di Security Lake per casi d'uso investigativi e di analisi.

Per attivare questa integrazione, è necessario abilitare entrambi i servizi e aggiungere Security Hub CSPM come origine nella console di Security Lake, nell'API Security Lake o. AWS CLI Una volta completati questi passaggi, Security Hub CSPM inizia a inviare tutti i risultati a Security Lake.

Security Lake normalizza automaticamente i risultati CSPM di Security Hub e li converte in uno schema open source standardizzato chiamato Open Cybersecurity Schema Framework (OCSF). In Security Lake, puoi aggiungere uno o più abbonati per utilizzare i risultati del Security Hub CSPM.

Per ulteriori informazioni su questa integrazione, comprese le istruzioni sull'aggiunta di Security Hub CSPM come origine e sulla creazione di abbonati, consulta Integration with AWS Security Hub CSPM nella Amazon Security Lake User Guide.

AWS Systems Manager Explorer e OpsCenter (riceve e aggiorna i risultati)

AWS Systems Manager Esplora e OpsCenter ricevi i risultati da Security Hub CSPM e aggiorna tali risultati in Security Hub CSPM.

Explorer offre una dashboard personalizzabile, che fornisce approfondimenti e analisi chiave sullo stato operativo e sulle prestazioni del tuo ambiente. AWS

OpsCenter offre una posizione centrale per visualizzare, esaminare e risolvere gli elementi di lavoro operativi.

Per ulteriori informazioni su Explorer e OpsCenter, vedere Gestione delle operazioni nella Guida AWS Systems Manager per l'utente.

AWS Trusted Advisor (Riceve i risultati)

Trusted Advisor si basa sulle migliori pratiche apprese servendo centinaia di migliaia di AWS clienti. Trusted Advisor ispeziona l' AWS ambiente e quindi formula raccomandazioni quando esistono opportunità per risparmiare denaro, migliorare la disponibilità e le prestazioni del sistema o contribuire a colmare le lacune di sicurezza.

Quando abiliti entrambi Trusted Advisor e Security Hub CSPM, l'integrazione viene aggiornata automaticamente.

Security Hub CSPM invia i risultati dei suoi controlli sulle migliori pratiche di sicurezza AWS fondamentali a. Trusted Advisor

Per ulteriori informazioni sull'integrazione di Security Hub CSPM con Trusted Advisor, vedere Visualizzazione dei controlli CSPM AWS di Security Hub nella Support AWS User AWS Trusted Advisor Guide.

Third-party integrazioni di prodotti con Security Hub CSPM

AWS Security Hub CSPM si integra con più prodotti partner di terze parti. Un'integrazione può eseguire una o più delle seguenti azioni:

- Invia i risultati generati a Security Hub CSPM

- Ricevi risultati da Security Hub CSPM
- Aggiorna i risultati in Security Hub CSPM

Le integrazioni che inviano i risultati a Security Hub CSPM hanno un Amazon Resource Name (ARN).

Un'integrazione potrebbe non essere completamente disponibile. Regioni AWS Se un'integrazione non è supportata nella regione a cui hai attualmente effettuato l'accesso sulla console CSPM di Security Hub, non viene visualizzata nella pagina Integrazioni della console. Per un elenco delle integrazioni disponibili nelle regioni della Cina e AWS GovCloud (US) Regions, consultaDisponibilità di integrazioni per regione.

`<Se disponi di una soluzione di sicurezza e sei interessato a diventare un partn`
Per ulteriori informazioni, consulta la Partner Integration Guide.

Panoramica delle integrazioni di terze parti con Security Hub CSPM

La tabella seguente fornisce una panoramica delle integrazioni di terze parti che possono inviare risultati a Security Hub CSPM o ricevere risultati da Security Hub CSPM.

Integrazione	Direzione	ARN (se applicabile)
3CORESec – 3CORESec NTA	Invia i risultati	`arn:aws:securityhub: <REGION>::product/3coresec/3coresec`
Alert Logic – SIEMless Threat Management	Invia i risultati	`arn:aws:securityhub: <REGION>:733251395267:product/alertlogic/althreatmanagement`
Aqua Security – Aqua Cloud Native Security Platform	Invia i risultati	`arn:aws:securityhub: <REGION>::product/aquasecurity/aquasecurity`
Aqua Security – Kube-bench	Invia i risultati	`arn:aws:securityhub: <REGION>::product/`

Integrazione	Direzione	ARN (se applicabile)
		aqua-security/kube-bench
Armor – Armor Anywhere	Invia i risultati	arn:aws:securityhub: *<REGION>*:679703615338:product/armor defense/armoranywhere
AttackIQ – AttackIQ	Invia i risultati	arn:aws:securityhub: *<REGION>*::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	Invia i risultati	arn:aws:securityhub: *<REGION>*:151784055945:product/barracuda/cloudsecurity guardian
BigID – BigID Enterprise	Invia i risultati	arn:aws:securityhub: *<REGION>*::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	Invia i risultati	arn:aws:securityhub: *<REGION>*::product/blue-hexagon/blue-hexagon-for-aws
Check Point – CloudGuard IaaS	Invia i risultati	arn:aws:securityhub: *<REGION>*:758245563457:product/checkpoint/cloudguard-iaas

Integrazione	Direzione	ARN (se applicabile)
Check Point – CloudGuard Posture Management	Invia i risultati	`arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc`
Claroty – xDome	Invia i risultati	`arn:aws:securityhub: <REGION>::product/claroty/xdome`
Cloud Storage Security—Antivirus for Amazon S3	Invia i risultati	`arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`
Contrast Security	Invia i risultati	`arn:aws:securityhub: <REGION>::product/contrast-security/security-assess`
CrowdStrike – CrowdStrike Falcon	Invia i risultati	`arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`
CyberArk – Privileged Threat Analytics	Invia i risultati	`arn:aws:securityhub: <REGION>:749430749651:product/cyberark/cyberark-pta`
Data Theorem – Data Theorem	Invia i risultati	`arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure`

Integrazione	Direzione	ARN (se applicabile)
Drata	Invia i risultati	`arn:aws:securityhub: <REGION>::product/drata/drata-integration`
Forcepoint – Forcepoint CASB	Invia i risultati	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb`
Forcepoint – Forcepoint Cloud Security Gateway	Invia i risultati	`arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway`
Forcepoint – Forcepoint DLP	Invia i risultati	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp`
Forcepoint – Forcepoint NGFW	Invia i risultati	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw`
Fugue – Fugue	Invia i risultati	`arn:aws:securityhub: <REGION>::product/fugue/fugue`

Integrazione	Direzione	ARN (se applicabile)
Guardicore – Centra 4.0	Invia i risultati	`arn:aws:securityhub: <REGION>::product/guardicore/guardicore`
HackerOne – Vulnerability Intelligence	Invia i risultati	`arn:aws:securityhub: <REGION>::product/hackerone/vulnerability-intelligence`
JFrog – Xray	Invia i risultati	`arn:aws:securityhub: <REGION>::product/jfrog/jfrog-xray`
Juniper Networks – vSRX Next Generation Firewall	Invia i risultati	`arn:aws:securityhub: <REGION>::product/juniper-networks/vsrx-next-generation-firewall`
k9 Security – Access Analyzer	Invia i risultati	`arn:aws:securityhub: <REGION>::product/k9-security/access-analyzer`
Lacework – Lacework	Invia i risultati	`arn:aws:securityhub: <REGION>::product/lacework/lacework`
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Invia i risultati	`arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

Integrazione	Direzione	ARN (se applicabile)
NETSCOUT – NETSCOUT Cyber Investigator	Invia i risultati	`arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator`
Orca Cloud Security Platform	Invia i risultati	`arn:aws:securityhub: <REGION>::product/orca-security/orca-security`
Palo Alto Networks – Prisma Cloud Compute	Invia i risultati	`arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise`
Palo Alto Networks – Prisma Cloud Enterprise	Invia i risultati	`arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock`
Plerion – Cloud Security Platform	Invia i risultati	`arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform`
Prowler – Prowler	Invia i risultati	`arn:aws:securityhub: <REGION>::product/prowler/prowler`
Qualys – Vulnerability Management	Invia i risultati	`arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm`

Integrazione	Direzione	ARN (se applicabile)
Rapid7 – InsightVM	Invia i risultati	`arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm`
SentinelOne – SentinelOne	Invia i risultati	`arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection`
Snyk	Invia i risultati	`arn:aws:securityhub: <region>::product/snyk/snyk`
Sonrai Security – Sonrai Dig	Invia i risultati	`arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig`
Sophos – Server Protection	Invia i risultati	`arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection`
StackRox – StackRox Kubernetes Security	Invia i risultati	`arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security`
Sumo Logic – Machine Data Analytics	Invia i risultati	`arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda`

Integrazione	Direzione	ARN (se applicabile)
Symantec – Cloud Workload Protection	Invia i risultati	`arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp`
Tenable – Tenable.io	Invia i risultati	`arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io`
Trend Micro – Cloud One	Invia i risultati	`arn:aws:securityhub: <REGION>::product/trend-micro/cloud-one`
Vectra – Cognito Detect	Invia i risultati	`arn:aws:securityhub: <REGION>:978576646331:product/vectra-ai/cognito-detect`
Wiz	Invia i risultati	`arn:aws:securityhub: <REGION>::product/wiz-security/wiz-security`
Atlassian - Jira Service Management	Riceve e aggiorna i risultati	Non applicabile
Atlassian - Jira Service Management Cloud	Riceve e aggiorna i risultati	Non applicabile
Atlassian – Opsgenie	Riceve i risultati	Non applicabile
Dynatrace	Riceve i risultati	Non applicabile
Elastic	Riceve i risultati	Non applicabile

Integrazione	Direzione	ARN (se applicabile)
Fortinet – FortiCNP	Riceve i risultati	Non applicabile
IBM – QRadar	Riceve i risultati	Non applicabile
Logz.io Cloud SIEM	Riceve i risultati	Non applicabile
MetricStream	Riceve i risultati	Non applicabile
MicroFocus – MicroFocus Arcsight	Riceve i risultati	Non applicabile
New Relic Vulnerability Management	Riceve i risultati	Non applicabile
PagerDuty – PagerDuty	Riceve i risultati	Non applicabile
Palo Alto Networks – Cortex XSOAR	Riceve i risultati	Non applicabile
Palo Alto Networks – VM-Series	Riceve i risultati	Non applicabile
Rackspace Technology – Cloud Native Security	Riceve i risultati	Non applicabile
Rapid7 – InsightConnect	Riceve i risultati	Non applicabile
RSA – RSA Archer	Riceve i risultati	Non applicabile
ServiceNow – ITSM	Riceve e aggiorna i risultati	Non applicabile
Slack – Slack	Riceve i risultati	Non applicabile
Splunk – Splunk Enterprise	Riceve i risultati	Non applicabile
Splunk – Splunk Phantom	Riceve i risultati	Non applicabile
ThreatModeler	Riceve i risultati	Non applicabile

Integrazione	Direzione	ARN (se applicabile)
Trellix – Trellix Helix	Riceve i risultati	Non applicabile
Caveonix – Caveonix Cloud	Invia e riceve i risultati	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`
Cloud Custodian – Cloud Custodian	Invia e riceve i risultati	`arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian`
DisruptOps, Inc. – DisruptOPS	Invia e riceve i risultati	`arn:aws:securityhub: <REGION>::product/disruptops-inc/disruptops`
Kion	Invia e riceve i risultati	`arn:aws:securityhub: <REGION>::product/cloudtamerio/cloudtamerio`
Turbot – Turbot	Invia e riceve i risultati	`arn:aws:securityhub: <REGION>:453761072151:product/turbot/turbot`

Third-party integrazioni che inviano i risultati a Security Hub CSPM

Le seguenti integrazioni di prodotti di partner di terze parti possono inviare i risultati a Security Hub CSPM. Security Hub CSPM trasforma i risultati nel AWS Security Finding Format.

3 CoreSEC – NTA SEC a 3 core

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/3coresec/3coresec`

3CORESecfornisce servizi di rilevamento gestiti sia per ambienti locali che per sistemi. AWS La loro integrazione con Security Hub CSPM consente la visibilità su minacce come malware, escalation dei privilegi, movimenti laterali e segmentazione impropria della rete.

Link al prodotto

Documentazione dei partner

Alert Logic – Gestione delle minacce senza SIEM

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

Ottieni il giusto livello di copertura: visibilità delle vulnerabilità e degli asset, rilevamento delle minacce e gestione degli incidenti e opzioni assegnate agli analisti SOC. AWS WAF

Link al prodotto

Documentazione dei partner

Aqua Security – Aqua Cloud Native Security Platform

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP)offre la sicurezza completa del ciclo di vita per le applicazioni basate su container e serverless, dalla pipeline agli ambienti di produzione in fase di esecuzione CI/CD .

Link al prodotto

Documentazione dei partner

Aqua Security – Kube-bench

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-benchè uno strumento open source che esegue il benchmark Kubernetes Center for Internet Security (CIS) nel tuo ambiente.

Link al prodotto

documentazione per i partner

Armor – Armor Anywhere

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhereoffre sicurezza e conformità gestite per AWS.

Link al prodotto

Documentazione dei partner

AttackIQ – AttackIQ

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platformemula un comportamento antagonistico reale in linea con il MITRE ATT&CK Framework per aiutare a convalidare e migliorare il livello di sicurezza generale.

Link al prodotto

Documentazione dei partner

Barracuda Networks – Cloud Security Guardian

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentryaiuta le organizzazioni a rimanere sicure durante la creazione di applicazioni e lo spostamento dei carichi di lavoro nel cloud pubblico.

AWS Link al Marketplace

Link al prodotto

BigID – BigID Enterprise

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

BigID Enterprise Privacy Management PlatformAiuta le aziende a gestire e proteggere i dati sensibili (PII) su tutti i loro sistemi.

Link al prodotto

Documentazione dei partner

Esagono blu – Esagono blu for AWS

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagonè una piattaforma di rilevamento delle minacce in tempo reale. Utilizza i principi del deep learning per rilevare minacce note e sconosciute, inclusi malware e anomalie di rete.

AWS Link al Marketplace

Documentazione dei partner

Punto di controllo – CloudGuard IaaS

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuardestende facilmente la sicurezza completa per la prevenzione delle minacce proteggendo al AWS contempo le risorse nel cloud.

Link al prodotto

Documentazione dei partner

Punto di controllo – CloudGuard Gestione della postura

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Una piattaforma SaaS che offre sicurezza di rete cloud verificabile, protezione IAM avanzata e conformità e governance complete.

Link al prodotto

Documentazione dei partner

Clarity – Cupola

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDomeaiuta le organizzazioni a proteggere i propri sistemi cyber-fisici attraverso l'Extended Internet of Things (XIoT) all'interno di ambienti industriali (OT), sanitari (IoMT) e aziendali (IoT).

Link al prodotto

Documentazione dei partner

Sicurezza dell'archiviazione nel cloud – Antivirus per Simple Storage Service (Amazon S3)

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Securityfornisce una scansione antimalware e antivirus nativa per il cloud per oggetti Amazon S3.

Antivirus for Amazon S3 offre scansioni pianificate e in tempo reale di oggetti e file in Amazon S3 alla ricerca di malware e minacce. Fornisce visibilità e risoluzione di problemi e file infetti.

Link al prodotto

Documentazione dei partner

Contrast Security — Contrast Assenti

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assessè uno strumento IAST che offre il rilevamento delle vulnerabilità in tempo reale in app Web, API e microservizi. Contrast Assesssi integra con Security Hub CSPM per contribuire a fornire visibilità e risposta centralizzate per tutti i carichi di lavoro.

Link al prodotto

Documentazione dei partner

CrowdStrike – CrowdStrike Falcon

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

Il sensore CrowdStrike Falcon unico e leggero unisce l'antivirus di nuova generazione, il rilevamento e la risposta degli endpoint e la caccia 24/7 gestita tramite il cloud.

AWS Link al Marketplace

Documentazione dei partner

CyberArk – Privileged Threat Analytics

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analyticsraccoglie, rileva, avvisa e rispondi alle attività e ai comportamenti ad alto rischio degli account privilegiati per contenere gli attacchi in corso.

Link al prodotto

Documentazione dei partner

Teorema dei dati – Teorema dei dati

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theoremanalizza continuamente applicazioni Web, API e risorse cloud alla ricerca di falle di sicurezza e lacune nella privacy dei dati per prevenire violazioni dei dati. AppSec

Link al prodotto

Documentazione dei partner

Dati

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drataè una piattaforma di automazione della conformità che consente di raggiungere e mantenere la conformità con vari framework, come SOC2, ISO e GDPR. L'integrazione tra Security Hub Drata e CSPM ti aiuta a centralizzare i risultati di sicurezza in un'unica posizione.

AWS Link al Marketplace

Documentazione dei partner

Forcepoint – Forcepoint CASB

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASBconsente di scoprire l'uso delle applicazioni cloud, analizzare i rischi e applicare controlli appropriati per SaaS e applicazioni personalizzate.

Link al prodotto

Documentazione dei partner

Forcepoint – Gateway di sicurezza cloud Forcepoint

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gatewayè un servizio di sicurezza cloud convergente che offre visibilità, controllo e protezione dalle minacce per utenti e dati, ovunque si trovino.

Link al prodotto

Documentazione dei partner

Forcepoint – Forcepoint DLP

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLPaffronta il rischio incentrato sull'uomo con visibilità e controllo ovunque lavorino i dipendenti e ovunque risiedano i dati.

Link al prodotto

documentazione per i partner

Forcepoint – Forcepoint NGFW

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFWconsente di connettere AWS l'ambiente alla rete aziendale con la scalabilità, la protezione e le informazioni necessarie per gestire la rete e rispondere alle minacce.

Link al prodotto

Documentazione dei partner

Fuga – Fuga

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugueè una piattaforma cloud-native scalabile e priva di agenti che automatizza la convalida continua degli ambienti infrastructure-as-code e cloud runtime utilizzando le stesse policy.

Link al prodotto

Documentazione dei partner

Guardicore – Centra 4.0

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centrafornisce la visualizzazione del flusso, la microsegmentazione e il rilevamento delle violazioni per i carichi di lavoro nei data center e nei cloud moderni.

Link al prodotto

Documentazione dei partner

HackerOne – Informazioni sulla vulnerabilità

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

La HackerOne piattaforma collabora con la comunità globale di hacker per scoprire i problemi di sicurezza più rilevanti. Vulnerability Intelligenceconsente all'organizzazione di andare oltre la scansione automatica. Condivide le vulnerabilità che gli hacker HackerOne etici hanno convalidato e fornito misure per riprodurre.

AWS link al marketplace

documentazione per i partner

JFrog – Radiografia

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xrayè uno strumento universale di analisi della composizione del software (SCA) per la sicurezza delle applicazioni che analizza continuamente i file binari per verificare la conformità delle licenze e le vulnerabilità di sicurezza, in modo da poter gestire una catena di fornitura software sicura.

AWS Link al Marketplace

Documentazione dei partner

Juniper Networks – Firewall vSRx di nuova generazione

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'vSRx Virtual Next Generation Firewall offre un firewall virtuale completo basato sul cloud con sicurezza avanzata, rete sicura SD-WAN e robusta e automazione integrata.

AWS Link al Marketplace

Documentazione dei partner

Link al prodotto

sicurezza k9 – Access Analyzer

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Securityti avvisa quando vengono apportate importanti modifiche all'accesso nel tuo AWS Identity and Access Management account. Conk9 Security, puoi comprendere l'accesso che gli utenti e i ruoli IAM hanno ai dati critici Servizi AWS e ai tuoi dati.

k9 Securityè progettato per la distribuzione continua e consente di rendere operativo IAM con audit di accesso attuabili e una semplice automazione delle politiche per e Terraform. AWS CDK

Link al prodotto

Documentazione dei partner

Merletti – Merletti

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Laceworkè la piattaforma di sicurezza basata sui dati per il cloud. La Lacework Cloud Security Platform automatizza la sicurezza del cloud su larga scala in modo da poter innovare con velocità e sicurezza.

Link al prodotto

Documentazione dei partner

McAfee – Piattaforma di protezione delle applicazioni native per il cloud (CNAPP) MVISION

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP)offre Cloud Security Posture Management (CSPM) e Cloud Workload Protection Platform (CWPP) per il tuo ambiente. AWS

Link al prodotto

documentazione per i partner

NETSCOUT – Investigatore informatico NETSCOUT

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigatorè una piattaforma di analisi forense, indagine sui rischi e analisi forense delle minacce di rete a livello aziendale che aiuta a ridurre l'impatto delle minacce informatiche sulle aziende.

Link al prodotto

Documentazione dei partner

Piattaforma di sicurezza Orca Cloud

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/orca-security/orca-security`

Orca Cloud Security PlatformIdentifica, assegna priorità e risolve i rischi e i problemi di conformità nell'intero ambiente cloud. Orca'sagentless-first, la AI-driven piattaforma offre una copertura completa rilevando vulnerabilità, configurazioni errate, movimenti laterali, rischi legati alle API, dati sensibili, eventi e comportamenti anomali e identità eccessivamente permissive.

Orcasi integra con Security Hub CSPM per portare la telemetria di sicurezza cloud approfondita in Security Hub CSPM. Orca, utilizzando la sua SideScanning tecnologia, dà priorità ai rischi nell'infrastruttura cloud, nei carichi di lavoro, nelle applicazioni, nei dati, nelle API, nelle identità e altro ancora.

Link al prodotto

Documentazione dei partner

Palo Alto Networks – Prisma Cloud Compute

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Computeè una piattaforma di sicurezza informatica nativa per il cloud che protegge VM, container e piattaforme serverless.

Link al prodotto

Documentazione dei partner

Palo Alto Networks – Prisma Cloud Enterprise

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Protegge la tua AWS implementazione con analisi della sicurezza nel cloud, rilevamento avanzato delle minacce e monitoraggio della conformità.

Link al prodotto

Documentazione dei partner

Plerion – Piattaforma di sicurezza cloud

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerionè una piattaforma di sicurezza cloud con un approccio unico basato sulle minacce e basato sul rischio che offre azioni preventive, investigative e correttive per tutti i carichi di lavoro. L'integrazione tra Security Hub Plerion e CSPM consente ai clienti di centralizzare e agire in base ai propri risultati di sicurezza in un unico posto.

AWS Link al Marketplace

Documentazione dei partner

che si aggira – che si aggira

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowlerè uno strumento di sicurezza open source per eseguire AWS controlli relativi alle migliori pratiche di sicurezza, al rafforzamento e al monitoraggio continuo.

Link al prodotto

documentazione per i partner

Qualys – Vulnerability Management

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM)analizza e identifica continuamente le vulnerabilità, proteggendo le tue risorse.

Link al prodotto

Documentazione dei partner

Rapid7 – InsightVM

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVMfornisce la gestione delle vulnerabilità per gli ambienti moderni, consentendoti di individuare, assegnare priorità e correggere in modo efficiente le vulnerabilità.

Link al prodotto

Documentazione dei partner

SentinelOne – SentinelOne

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOneè una piattaforma autonoma di rilevamento e risposta estesa (XDR) che comprende AI-powered prevenzione, rilevamento, risposta e caccia su endpoint, container, carichi di lavoro cloud e dispositivi IoT.

AWS Link al Marketplace

Link al prodotto

Snyk

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snykfornisce una piattaforma di sicurezza che analizza i componenti delle app alla ricerca di rischi per la sicurezza nei carichi di lavoro in esecuzione. AWS Questi rischi vengono inviati a Security Hub

CSPM come risultati, aiutando gli sviluppatori e i team di sicurezza a visualizzarli e assegnare loro priorità insieme al resto dei risultati di sicurezza. AWS

AWS Link al Marketplace

Documentazione dei partner

Sicurezza del Sonari – Sonrai Dig

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Digmonitora e corregge le configurazioni errate del cloud e le violazioni delle policy, in modo da poter migliorare il livello di sicurezza e conformità.

Link al prodotto

Documentazione dei partner

Sophos – Server Protection

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protectiondifende le applicazioni e i dati critici alla base dell'organizzazione, utilizzando tecniche complete di difesa in profondità.

Link al prodotto

StackRox – StackRox Sicurezza Kubernetes

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRoxaiuta le aziende a proteggere le implementazioni di container e Kubernetes su larga scala applicando le politiche di conformità e sicurezza durante l'intero ciclo di vita dei container: creazione, implementazione ed esecuzione.

Link al prodotto

Documentazione dei partner

Sumo Logic – Machine Data Analytics

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logicè una piattaforma di analisi dei dati automatici sicura che consente ai team operativi di sviluppo e sicurezza di creare, eseguire e proteggere AWS le proprie applicazioni.

Link al prodotto

Documentazione dei partner

Symantec – Cloud Workload Protection

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protectionfornisce una protezione completa per le tue istanze Amazon EC2 con antimalware, prevenzione delle intrusioni e monitoraggio dell'integrità dei file.

Link al prodotto

Documentazione dei partner

Tenable – Tenable.io

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Identifica, analizza e definisce la priorità delle vulnerabilità. Gestito nel cloud.

Link al prodotto

Documentazione dei partner

Trend Micro – Cloud One

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud Onefornisce le informazioni di sicurezza giuste ai team nel momento e nel luogo giusti. Questa integrazione invia i risultati di sicurezza a Security Hub CSPM in tempo reale, migliorando la visibilità AWS delle risorse e dei dettagli Trend Micro Cloud One degli eventi in Security Hub CSPM.

AWS Link al Marketplace

Documentazione dei partner

Vectra – Rilevamento Cognito

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectrasta trasformando la sicurezza informatica applicando l'intelligenza artificiale avanzata per rilevare e rispondere agli aggressori informatici nascosti prima che possano rubare o causare danni.

AWS Link al Marketplace

Documentazione dei partner

Wiz – Wiz Security

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wizanalizza continuamente configurazioni, vulnerabilità, reti, impostazioni IAM, segreti e altro ancora tra utenti e carichi di lavoro per scoprire problemi critici che rappresentano un rischio effettivo. Account AWS Integra Wiz con Security Hub CSPM per visualizzare e rispondere ai problemi rilevati da Wiz dalla console CSPM di Security Hub.

AWS Link al Marketplace

Documentazione dei partner

Third-party integrazioni che ricevono risultati da Security Hub CSPM

Le seguenti integrazioni di prodotti di partner di terze parti possono ricevere i risultati dal Security Hub CSPM. Dove indicato, il prodotto potrebbe anche aggiornare i risultati. In questo caso, gli aggiornamenti apportati ai risultati del prodotto partner si riflettono anche in Security Hub CSPM.

Atlassian - Gestione dei servizi Jira

Tipo di integrazione: ricezione e aggiornamento

Il AWS Service Management Connector for Jira invia i risultati dal Security Hub CSPM a. Jira Jirai problemi vengono creati sulla base dei risultati. Quando i Jira problemi vengono aggiornati, i risultati corrispondenti vengono aggiornati in Security Hub CSPM.

L'integrazione supporta solo Jira Server e Jira Data Center.

Per una panoramica dell'integrazione e di come funziona, guarda il video AWS Security Hub CSPM — Integrazione bidirezionale con. Atlassian Jira Service Management

Link al prodotto

Documentazione dei partner

Atlassian - Jira Service Management Cloud

Tipo di integrazione: ricezione e aggiornamento

Jira Service Management Cloudè il componente cloud di Jira Service Management.

Il AWS Service Management Connector for Jira invia i risultati dal Security Hub CSPM a. Jira I risultati innescano la creazione di problemi in. Jira Service Management Cloud Quando aggiorni questi problemi inJira Service Management Cloud, i risultati corrispondenti vengono aggiornati anche in Security Hub CSPM.

Link al prodotto

Documentazione dei partner

Atlassian – Opsgenie

Tipo di integrazione: Ricevere

Opsgenieè una moderna soluzione di gestione degli incidenti per la gestione di servizi sempre attivi, che consente ai team di sviluppo e operativi di pianificare le interruzioni del servizio e mantenere il controllo durante gli incidenti.

L'integrazione con Security Hub CSPM garantisce che gli incidenti di sicurezza mission critical vengano indirizzati ai team appropriati per una risoluzione immediata.

Link al prodotto

Documentazione dei partner

Dynatrace

Tipo di integrazione: ricezione

L'Dynatraceintegrazione con Security Hub CSPM aiuta a unificare, visualizzare e automatizzare i risultati di sicurezza tra strumenti e ambienti. L'aggiunta Dynatrace di un contesto di runtime ai risultati di sicurezza consente una definizione delle priorità più intelligente, aiuta a ridurre il rumore causato dagli avvisi e consente ai DevSecOps team di porre rimedio in modo efficiente ai problemi critici che riguardano gli ambienti e le applicazioni di produzione.

Link al prodotto

Documentazione dei partner

Elastic

Tipo di integrazione: ricezione

Elasticcrea soluzioni basate sulla ricerca per la sicurezza, l'osservabilità e la ricerca. Grazie all'integrazione con Security Hub CSPM, Elastic acquisisce in modo programmatico i risultati e le informazioni da Security Hub CSPM, li normalizza per la correlazione e l'analisi e presenta dashboard e rilevamenti unificati, consentendo un triage e un'indagine più rapidi senza l'impiego di agenti. Elastic Security

Link al prodotto

Documentazione dei partner

Fortinet – FortiCNP

Tipo di integrazione: ricezione

FortiCNPè un prodotto Cloud Native Protection che aggrega i risultati sulla sicurezza in informazioni fruibili e dà priorità alle informazioni sulla sicurezza in base al punteggio di rischio per ridurre l'affaticamento degli avvisi e accelerare la correzione.

AWS Link al Marketplace

Documentazione dei partner

IBM – QRadar

Tipo di integrazione: ricezione

IBM QRadarSIEM offre ai team di sicurezza la capacità di rilevare, assegnare priorità, indagare e rispondere alle minacce in modo rapido e preciso.

Link al prodotto

Documentazione dei partner

Logz.io SIEM cloud

Tipo di integrazione: ricezione

Logz.ioè un fornitore Cloud SIEM che fornisce una correlazione avanzata di dati di log ed eventi per aiutare i team di sicurezza a rilevare, analizzare e rispondere alle minacce alla sicurezza in tempo reale.

Link al prodotto

Documentazione dei partner

MetricStream – CyberGRC

Tipo di integrazione: ricezione

MetricStream CyberGRCti aiuta a gestire, misurare e mitigare i rischi di sicurezza informatica. Ricevendo i risultati del Security Hub CSPM, CyberGRC offre una maggiore visibilità su questi rischi, in modo da poter dare priorità agli investimenti in sicurezza informatica e rispettare le politiche IT.

AWS Link al Marketplace

Link al prodotto

MicroFocus – MicroFocus Arcsight

Tipo di integrazione: Ricevere

ArcSightaccelera il rilevamento e la risposta efficaci alle minacce in tempo reale, integrando la correlazione degli eventi e l'analisi supervisionata e non supervisionata con l'automazione e l'orchestrazione della risposta.

Link al prodotto

Documentazione dei partner

Gestione delle vulnerabilità di New Relic

Tipo di integrazione: ricezione

New Relic Vulnerability Managementriceve i risultati di sicurezza da Security Hub CSPM, in modo da poter ottenere una visione centralizzata della sicurezza insieme alla telemetria delle prestazioni nel contesto dell'intero stack.

AWS Link al Marketplace

Documentazione dei partner

PagerDuty – PagerDuty

Tipo di integrazione: ricezione

La piattaforma di gestione delle operazioni PagerDuty digitali consente ai team di mitigare in modo proattivo i problemi che hanno un impatto sui clienti trasformando automaticamente qualsiasi segnale in informazioni e azioni corrette.

AWS gli utenti possono utilizzare il PagerDuty set di AWS integrazioni per scalare i propri ambienti ibridi con sicurezza. AWS

Se abbinato agli avvisi di sicurezza aggregati e organizzati di Security Hub CSPM, PagerDuty consente ai team di automatizzare il processo di risposta alle minacce e di impostare rapidamente azioni personalizzate per prevenire potenziali problemi.

PagerDutygli utenti che stanno intraprendendo un progetto di migrazione al cloud possono agire rapidamente, riducendo al contempo l'impatto dei problemi che si verificano durante il ciclo di vita della migrazione.

Link al prodotto

Documentazione dei partner

Palo Alto Networks – Cortex XSOAR

Tipo di integrazione: Ricevere

Cortex XSOARè una piattaforma SOAR (Security Orchestration, Automation and Response) che si integra con l'intero stack di prodotti di sicurezza per accelerare la risposta agli incidenti e le operazioni di sicurezza.

Link al prodotto

Documentazione dei partner

Palo Alto Networks – VM-Series

Tipo di integrazione: ricezione

Palo Alto VM-Seriesl'integrazione con Security Hub CSPM raccoglie informazioni sulle minacce e le invia al firewall di VM-Series nuova generazione come aggiornamento automatico della politica di sicurezza che blocca le attività dannose degli indirizzi IP.

Link al prodotto

documentazione per i partner

Tecnologia Rackspace – Sicurezza nativa nel cloud

Tipo di integrazione: Ricevere

Rackspace Technology fornisce servizi di sicurezza gestiti oltre a prodotti di AWS sicurezza nativi per il monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni l'anno tramite Rackspace SOC, l'analisi avanzata e la risoluzione delle minacce.

Link al prodotto

Rapid7 – InsightConnect

Tipo di integrazione: Ricevere

Rapid7 InsightConnectè una soluzione di orchestrazione e automazione della sicurezza che consente al team di ottimizzare le operazioni SOC con poco o nessun codice.

Link al prodotto

Documentazione dei partner

RSA – RSA Archer

Tipo di integrazione: Receive

RSA ArcherLa gestione dei rischi IT e di sicurezza consente di determinare quali risorse sono fondamentali per l'azienda, stabilire e comunicare politiche e standard di sicurezza, rilevare e rispondere agli attacchi, identificare e correggere le carenze di sicurezza e stabilire chiare best practice di gestione del rischio IT.

Link al prodotto

Documentazione dei partner

ServiceNow – ITSM

Tipo di integrazione: ricezione e aggiornamento

L'ServiceNowintegrazione con Security Hub CSPM consente di visualizzare i risultati di sicurezza di Security Hub CSPM all'interno. ServiceNow ITSM Puoi anche configurare ServiceNow per creare automaticamente un incidente o un problema quando riceve un risultato dal Security Hub CSPM.

Qualsiasi aggiornamento a questi incidenti e problemi comporta l'aggiornamento dei risultati in Security Hub CSPM.

Per una panoramica dell'integrazione e di come funziona, guarda il video AWS Security Hub CSPM - Integrazione bidirezionale con. ServiceNow ITSM

Link al prodotto

Documentazione dei partner

Slack – Slack

Tipo di integrazione: ricezione

Slackè un livello dello stack tecnologico aziendale che riunisce persone, dati e applicazioni. Si tratta di un unico luogo in cui le persone possono collaborare in modo efficiente, trovare informazioni importanti e accedere a centinaia di migliaia di applicazioni e servizi critici per svolgere al meglio il loro lavoro.

Link al prodotto

documentazione per i partner

Splunk – Splunk Enterprise

Tipo di integrazione: ricezione

Splunkutilizza Amazon CloudWatch Events come consumatore dei risultati CSPM di Security Hub. Invia i tuoi dati a Splunk per analisi di sicurezza avanzate e SIEM.

Link al prodotto

Documentazione dei partner

Splunk – Splunk Phantom

Tipo di integrazione: ricezione

Con l'Splunk Phantomapplicazione per AWS Security Hub CSPM, i risultati vengono inviati Phantom per l'arricchimento automatico del contesto con informazioni aggiuntive sulla threat intelligence o per eseguire azioni di risposta automatizzate.

Link al prodotto

Documentazione dei partner

ThreatModeler

Tipo di integrazione: ricezione

ThreatModelerè una soluzione di modellazione automatizzata delle minacce che protegge e ridimensiona il ciclo di vita del software aziendale e dello sviluppo del cloud.

Link al prodotto

documentazione per i partner

Trellix – Trellix Helix

Tipo di integrazione: Ricevere

Trellix Helixè una piattaforma operativa di sicurezza ospitata nel cloud che consente alle organizzazioni di assumere il controllo di qualsiasi incidente, dall'avviso alla risoluzione.

Link al prodotto

Documentazione dei partner

Third-party integrazioni che inviano e ricevono risultati da Security Hub CSPM

Le seguenti integrazioni di prodotti di partner di terze parti possono inviare e ricevere risultati da Security Hub CSPM.

Caveonix – Caveonix Cloud

Tipo di integrazione: invio e ricezione

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

La Caveonix AI-powered piattaforma automatizza la visibilità, la valutazione e la mitigazione nei cloud ibridi, coprendo servizi, VM e container nativi del cloud. Integrato con AWS Security Hub CSPM, Caveonix unisce AWS dati e analisi avanzate per approfondire gli avvisi di sicurezza e la conformità.

AWS Link al Marketplace

Documentazione dei partner

Cloud Custodian – Cloud Custodian

Tipo di integrazione: invio e ricezione

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodianconsente agli utenti di essere ben gestiti nel cloud. Il semplice YAML DSL consente regole facilmente definite per consentire un'infrastruttura cloud ben gestita, sicura e ottimizzata in termini di costi.

Link al prodotto

Documentazione dei partner

DisruptOps, Inc. – DisruptOPS

Tipo di integrazione: invio e ricezione

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

La DisruptOps Security Operations Platform aiuta le organizzazioni a mantenere le migliori pratiche di sicurezza nel cloud attraverso l'uso di guardrail automatizzati.

Link al prodotto

Documentazione dei partner

Kion

Tipo di integrazione: invio e ricezione

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(precedentemente cloudtamer.io) è una soluzione completa di governance del cloud per. AWSKionoffre alle parti interessate visibilità sulle operazioni cloud e aiuta gli utenti del cloud a gestire gli account, controllare budget e costi e garantire la conformità continua.

Link al prodotto

Documentazione dei partner

Turbot – Turbot

Tipo di integrazione: invio e ricezione

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbotgarantisce che la tua infrastruttura cloud sia sicura, conforme, scalabile e ottimizzata in termini di costi.

Link al prodotto

Documentazione dei partner

Integrazione di Security Hub CSPM con prodotti personalizzati

Oltre ai risultati generati da AWS servizi integrati e prodotti di terze parti, AWS Security Hub CSPM può utilizzare i risultati generati da altri prodotti di sicurezza personalizzati.

È possibile inviare questi risultati a Security Hub CSPM utilizzando il BatchImportFindingsfunzionamento dell'API CSPM di Security Hub. Puoi utilizzare la stessa

operazione per aggiornare i risultati dei prodotti personalizzati che hai già inviato a Security Hub CSPM.

Quando configuri l'integrazione personalizzata, utilizza le linee guida e le liste di controllo fornite nella Security Hub CSPM Partner Integration Guide.

Requisiti e consigli per integrazioni di prodotti personalizzate

Prima di poter richiamare correttamente l'operazione `BatchImportFindings`API, è necessario abilitare Security Hub CSPM.

È inoltre necessario fornire i dettagli di ricerca per il prodotto personalizzato utilizzando il. the section called "Formato di ricerca: ASFF" Consulta i seguenti requisiti e consigli per le integrazioni di prodotti personalizzati:

Impostazione dell'ARN del prodotto

Quando abiliti Security Hub CSPM, nel tuo account corrente viene generato un prodotto Amazon Resource Name (ARN) predefinito per Security Hub CSPM.

Questo ARN del prodotto ha il seguente formato: `arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`. Ad esempio, `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`.

Utilizza questo ARN del prodotto come il valore per l'attributo `ProductArn` quando richiami l'operazione API `BatchImportFindings`.

Impostazione dei nomi dell'azienda e dei prodotti

È possibile utilizzare `BatchImportFindings` per impostare un nome aziendale e un nome di prodotto preferiti per l'integrazione personalizzata che invia i risultati a Security Hub CSPM.

I nomi specificati sostituiscono il nome dell'azienda e il nome del prodotto preconfigurati, denominati rispettivamente nome personale e nome predefinito, e vengono visualizzati nella console CSPM di Security Hub e nel codice JSON di ogni risultato. Consulta BatchImportFindings per trovare fornitori.

Impostazione degli ID risultato

È necessario fornire, gestire e incrementare gli ID risultato, utilizzando l'attributo `Id`.

Ogni nuovo risultato deve avere un ID di ricerca univoco. Se il prodotto personalizzato invia più risultati con lo stesso ID di ricerca, Security Hub CSPM elabora solo il primo risultato.

Impostazione dell'ID account

È necessario specificare il proprio ID account, utilizzando l'attributo `AwsAccountId`.

Impostazione delle date di creazione e aggiornamento

È necessario fornire i propri timestamp per gli attributi `CreatedAt` e `UpdatedAt`.

Aggiornamento dei risultati da prodotti personalizzati

Oltre a inviare nuovi risultati da prodotti personalizzati, puoi anche aggiornare i risultati esistenti di prodotti personalizzati utilizzando l'operazione API `BatchImportFindings`.

Per aggiornare i risultati esistenti, utilizza l'ID risultato esistente (tramite l'attributo `Id`). Invia nuovamente il risultato completo con le informazioni appropriate aggiornate nella richiesta, incluso un timestamp `UpdatedAt` modificato.

Esempio di integrazioni personalizzate

È possibile utilizzare il seguente esempio di integrazioni di prodotti personalizzati come guida per creare soluzioni personalizzate:

Invio dei risultati delle Chef InSpec scansioni al Security Hub CSPM

È possibile creare un CloudFormation modello che esegua una scansione di Chef InSpec conformità e quindi invii i risultati a Security Hub CSPM.

Per maggiori dettagli, consulta Monitoraggio continuo della conformità con Chef InSpecAWS Security Hub CSPM.

Invio di vulnerabilità dei container rilevate da Trivy Security Hub CSPM

È possibile creare un CloudFormation modello da utilizzare per AquaSecurity Trivy scansionare i contenitori alla ricerca di vulnerabilità e quindi inviare tali risultati di vulnerabilità a Security Hub CSPM.

Per maggiori dettagli, vedi Come creare una CI/CD pipeline per la scansione delle vulnerabilità dei container con TrivyAWS Security Hub CSPM.

Integrazione del Security Hub CSPM con Microsoft Azure

Per monitorare le tue risorse Microsoft Azure, puoi integrare Microsoft Azure con AWS Security Hub CSPM. Security Hub CSPM abilita quindi automaticamente i controlli di gestione della postura per l'ambiente Azure e genera risultati sull'ambiente. Più specificamente, il servizio offre quanto segue:

> **Note**
>
> Puoi gestire gli standard e i controlli di Azure usando la console CSPM di Security Hub, le API e. AWS CloudFormation La funzionalità Security Hub CSPM Central Configuration non è supportata per gli standard di Azure.

- Risultati ASFF: Security Hub CSPM genera i risultati nel formato AWS Security Finding Format (ASFF) per i controlli posturali che esegue per le risorse di Azure.
- CIS Microsoft Azure Foundations Benchmark v4.0: controlli di conformità automatizzati rispetto allo standard CIS Azure v4.0. Questo standard include controlli di identità, rete, archiviazione, registrazione e database.
- Best practice di Azure Foundational: rilevamento automatico di configurazioni errate delle risorse di Azure basato su best practice di sicurezza AWS curate che riguardano la sicurezza di rete, la gestione delle identità, la protezione dei dati e la registrazione.
- Gestione della postura: valutazione continua delle configurazioni delle risorse di Azure rispetto alle best practice di sicurezza e agli standard di conformità, con 122 controlli per entrambi gli standard.
- Per-provider Punteggi di sicurezza: separa i punteggi di sicurezza per Azure AWS e Azure, in modo da poter monitorare ogni ambiente in modo indipendente.

Per creare l'integrazione, connetti il tuo ambiente Azure a Security Hub CSPM tramite la seguente procedura:

> **Note**
>
> Gli standard di Azure differiscono dagli AWS standard nei seguenti modi:
>
> - Gli standard di Azure non richiedono prerequisiti manuali AWS Config . A differenza dei AWS casi in cui CSPM-only i clienti necessitano di un registratore gestito dal cliente, gli standard di Azure usano automaticamente un registratore interno collegato al servizio.

- Gli standard di Azure usano sempre regole di configurazione interne collegate ai servizi. AWS gli standard utilizzano regole di configurazione collegate ai servizi solo quando è abilitato anche Security Hub.

1. Puoi configurare il tuo ambiente Azure con una registrazione dell'applicazione, credenziali di identità federate, assegnazioni di ruoli di Azure e un'infrastruttura Event Hub.
2. Utilizzando la console Security Hub CSPM, si crea un connettore per l'integrazione. Devi specificare l'ID del tenant di Azure, l'ID client dell'applicazione e l'ambito di monitoraggio.
3. AWS Config raccoglie i dati di configurazione delle risorse dal tuo ambiente Azure.

   AWS Config viene utilizzato internamente per raccogliere dati di configurazione delle risorse. A differenza della gestione della AWS postura, in cui è necessario abilitare AWS Config e pagare in modo esplicito la registrazione, la gestione della postura di Azure viene gestita automaticamente. AWS Config Non è necessario abilitarlo AWS Config separatamente, configurare un registratore o pagare separatamente per l'utilizzo. AWS Config Questi costi sono inclusi nei prezzi CSPM di Security Hub.
4. Security Hub CSPM inizia a ricevere i dati di configurazione delle risorse e gli eventi del registro delle attività dall'ambiente Azure.
5. Security Hub CSPM genera risultati sulla gestione della postura relativi all'ambiente Azure.

In che modo AWS Config viene utilizzato

AWS Config viene usato internamente per raccogliere dati di configurazione delle risorse e rilevare le modifiche nell'ambiente Azure. Il connettore lo gestisce automaticamente. Non è necessario abilitarlo AWS Config separatamente, configurare un registratore o pagarne l' AWS Config utilizzo. Questi costi sono inclusi nei prezzi CSPM di Security Hub per le risorse di Azure.

Service-linked connettori e connettori gestiti dal cliente

Security Hub CSPM supporta due tipi di connettori:

Service-linked connettore (SLC)

Creato automaticamente quando configuri l'integrazione di Azure in Security Hub. L'ambito di un connettore collegato al servizio corrisponde sempre all'ambito definito nel connettore Security

Hub. Non è possibile modificare direttamente l'ambito di un connettore collegato al servizio; è invece possibile modificare l'ambito in Security Hub. Security Hub gestisce il ciclo di vita dei connettori collegati ai servizi per tuo conto.

Customer-managed connettore (CMC)

Creato direttamente nella console CSPM di Security Hub nella pagina Integrazioni. Utilizza un connettore gestito dal cliente quando desideri utilizzare Security Hub CSPM indipendentemente da Security Hub o quando hai bisogno di un ambito diverso dal connettore Security Hub. Quando esistono entrambi i tipi, l'ambito del connettore collegato al servizio deve essere sempre uguale o più ampio dell'ambito del connettore gestito dal cliente.

> **Note**
>
> A differenza di Security Hub, Security Hub CSPM non offre una selezione per funzionalità per i connettori di Azure. Quando si crea un connettore in Security Hub CSPM, tutte le funzionalità di gestione della postura vengono abilitate insieme.

Per informazioni sulla stima e il calcolo dei costi per l'integrazione di Security Hub CSPM con Azure, vedi i prezzi di Security AWS Hub CSPM.

Argomenti

- Prerequisiti per l'integrazione di Security Hub CSPM con Microsoft Azure
- Configurazione di Microsoft Azure per l'integrazione con Security Hub CSPM
- Configurazione del Security Hub CSPM per l'integrazione con Microsoft Azure
- Eliminazione di un connettore Microsoft Azure in Security Hub CSPM

Prerequisiti per l'integrazione di Security Hub CSPM con Microsoft Azure

Prima di integrare Microsoft Azure con AWS Security Hub CSPM, completa le seguenti attività nel tuo ambiente AWS e in Azure. Questo aiuta a garantire che tu e Security Hub CSPM disponiate delle risorse e delle autorizzazioni necessarie per monitorare le risorse di Azure.

Argomenti

- Prerequisiti per AWS

- Prerequisiti per Microsoft Azure

Prerequisiti per AWS

Verifica di avere quanto segue nel tuo Account AWS:

AWS Security Hub CSPM abilitato

Security Hub CSPM deve essere abilitato nel Account AWS e Regione AWS dove si desidera creare il connettore.

Autorizzazioni IAM della console

Il principale IAM che crea il connettore deve disporre delle seguenti autorizzazioni:

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

IAM Outbound Identity Federation è abilitata

Devi abilitare IAM Outbound Identity Federation nel tuo. Account AWS Questa funzionalità consente ai AWS servizi di autenticarsi presso provider di identità esterni (come Microsoft Entra ID) utilizzando credenziali federate anziché segreti di lunga durata.

Dopo aver abilitato Outbound Identity Federation, annota l'URL dell'emittente del token. Questo URL segue il formato:

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

Questo URL ti servirà per configurare le credenziali di identità federata in Azure.

Prerequisiti per Microsoft Azure

Verifica di avere quanto segue nel tuo ambiente Azure:

Tenant di Azure

È necessario disporre di un tenant di Azure nel cloud commerciale di Azure. Azure per enti pubblici e Azure Cina non sono supportati.

Disponibilità del registro ID Microsoft Entra

La registrazione delle risorse richiede i registri di controllo di Microsoft Graph e i registri di accesso del tenant Microsoft Entra ID. Alcuni registri ID Microsoft Entra richiedono licenze Microsoft Entra ID P1 o P2.

Se il tenant non dispone dei registri richiesti, la registrazione delle risorse potrebbe riportare errori parziali. La registrazione dell'app e le assegnazioni dei ruoli di Azure non forniscono dati di registro mancanti.

Ruolo di amministratore globale

La persona che configura l'ambiente Azure deve avere il ruolo di amministratore globale in Microsoft Entra ID. Questo ruolo è necessario per registrare le applicazioni, concedere il consenso dell'amministratore per le autorizzazioni dell'API Microsoft Graph, assegnare ruoli RBAC nell'ambito del gruppo di gestione principale del tenant e configurare le impostazioni diagnostiche per i registri di controllo Entra ID.

> **Note**
>
> In molte organizzazioni, l'amministratore globale di Azure e l'amministratore della sicurezza sono persone diverse. AWS La configurazione di Azure può essere completata indipendentemente utilizzando lo script di configurazione generato.

Registrazione dell'app Azure

È necessario registrare un'applicazione in Microsoft Entra ID. Questa applicazione funge da identità da AWS utilizzare per l'autenticazione nell'ambiente Azure utilizzando credenziali federate. Non sono richiesti segreti relativi ai clienti.

Hub per eventi di Azure

È necessario creare uno spazio dei nomi di Azure Event Hub e un'istanza Event Hub per ricevere gli eventi Activity Log e Entra ID Audit Log. Lo script di configurazione automatizza questa creazione.

Autorizzazioni dell'API Microsoft Graph

L'applicazione registrata richiede le seguenti autorizzazioni dell'API Microsoft Graph (tipo di applicazione, richiede il consenso dell'amministratore):

- `Directory.Read.All`— Leggi i dati delle directory, inclusi utenti, gruppi e responsabili dei servizi.
- `AuditLog.Read.All`— Leggi gli eventi del registro di controllo Entra ID.
- `Policy.Read.All`— Leggi le politiche dell'organizzazione e le configurazioni di accesso condizionale.

Ruolo di Azure RBAC Reader

Al responsabile del servizio deve essere assegnato il ruolo Reader nell'ambito del gruppo di gestione principale del tenant. Ciò garantisce l'accesso in sola lettura a tutte le risorse di Azure in tutte le sottoscrizioni del tenant.

Dopo aver completato queste attività, sei pronto per configurare il tuo ambiente Azure.

Configurazione di Microsoft Azure per l'integrazione con Security Hub CSPM

Dopo aver completato le attività relative ai prerequisiti, puoi configurare il tuo ambiente Microsoft Azure per supportare l'integrazione con AWS Security Hub CSPM. Per aiutarti a farlo, la console Security Hub CSPM genera uno script di configurazione personalizzato per la tua configurazione.

Per generare lo script, procedi come segue:

1. Aprire la console CSPM di Security Hub.
2. Nel riquadro di navigazione, scegli Integrazioni.
3. Scegli Crea connettore Azure.
4. Completa la configurazione del connettore (ID del tenant, ambito e nome), quindi copia lo script di configurazione generato.

Per eseguire lo script, usa l'interfaccia della riga di comando di Azure ed esegui l'autenticazione con un account Global Administrator (). `az login`

Quando esegui lo script, esegue una serie di attività. Le sezioni seguenti descrivono ogni operazione eseguita dallo script. Se l'organizzazione limita l'esecuzione degli script, è possibile eseguire queste attività manualmente, utilizzando questo argomento come guida. Dopo aver configurato l'ambiente Azure, puoi configurare Security Hub CSPM per l'integrazione con Azure.

> **Note**
>
> Una singola registrazione di un'app di Azure è condivisa tra i servizi di sicurezza. AWS Se usi anche Security Hub o Amazon Inspector for Azure, utilizzano la stessa registrazione dell'app. Non è necessario creare registrazioni separate per ogni servizio. AWS

Processi

- Passaggio 1: registrare un'applicazione Azure
- Fase 2: Creare un'entità del servizio
- Fase 3: Configurare le credenziali di identità federate
- Fase 4: Assegnazione del ruolo Reader
- Passaggio 5: configurare le autorizzazioni dell'API Microsoft Graph
- Passaggio 6: configura Azure Event Hub
- Passaggio 7: configurazione del registro delle attività e dell'esportazione del registro di controllo Entra ID

Passaggio 1: registrare un'applicazione Azure

Registra una nuova applicazione in Microsoft Entra ID. Questa applicazione funge da identità AWS utilizzata per l'autenticazione nell'ambiente Azure utilizzando credenziali federate. Non sono richiesti i segreti del cliente.

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

Annota l'ID dell'applicazione (client) dall'output (l'`appId`attributo). Questo valore verrà fornito durante la creazione del connettore nella console CSPM di Security Hub.

Fase 2: Creare un'entità del servizio

Creare un'entità di servizio per l'applicazione registrata. Si utilizzano le assegnazioni di ruolo di Azure per concedere le autorizzazioni all'entità del servizio. Il responsabile del servizio esegue azioni nel tuo ambiente Azure.

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

*application-client-id*Dov'è l'ID dell'applicazione (client) del passaggio precedente.

Fase 3: Configurare le credenziali di identità federate

Configurare le credenziali di identità federate sull'applicazione per consentire l'autenticazione senza segreti del AWS cliente. Questo stabilisce un trust OIDC tra Azure e Azure. AWS Non vengono archiviati segreti o credenziali di lunga durata.

```
$ 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"
  }'
```

Valori chiave:

- Emittente: l'URL dell'emittente del token fornito da IAM Outbound Identity Federation. Segue il formato. `https://uuid.tokens.sts.global.api.aws`
- Oggetto: l'ARN del ruolo `AWSServiceRoleForConfigThirdParty` collegato al servizio nel tuo. Account AWS AWS crea automaticamente questo ruolo collegato al servizio durante la configurazione del connettore.
- Destinatari: `api://AzureADTokenExchange` (valore standard per la federazione delle identità dei carichi di lavoro).

Fase 4: Assegnazione del ruolo Reader

Assegna il ruolo Reader all'entità del servizio nell'ambito principale (`/`). Ciò garantisce l'accesso in sola lettura a tutte le risorse di Azure in tutte le sottoscrizioni del tenant.

> **Assegna Reader all'ambito principale**
>
> Assicuratevi di assegnare il ruolo Reader nell'ambito principale (`/`), non nell'ambito del gruppo di gestione principale del tenant. Security Hub CSPM legge le risorse di Azure per l'assegnazione dei ruoli in ogni ambito, incluse le assegnazioni con ambito nella radice del

tenant. Un'assegnazione Reader nel gruppo di gestione principale non copre le assegnazioni il cui scopo è/, quindi senza di essa tali letture hanno esito negativo con un errore di autorizzazione e il connettore può entrare in uno stato degradato.

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

Root-scope l'assegnazione richiede un accesso elevato

L'assegnazione di un ruolo nell'ambito principale (/) richiede un accesso elevato. Se l'assegnazione di un ruolo non riesce, verifica che la gestione degli accessi per le risorse di Azure sia impostata su Sì in Microsoft Entra ID > Proprietà. Quindi esci e accedi nuovamente per aggiornare il token.

Rimuovi l'elevazione temporanea della radice

L'abilitazione della gestione degli accessi per le risorse di Azure concede all'amministratore che ha effettuato l'accesso il ruolo di amministratore dell'accesso utente nell'ambito principale (/), che può gestire l'accesso in ogni sottoscrizione e gruppo di gestione del tenant. Una volta completato l'onboarding, imposta la gestione degli accessi per le risorse di Azure su No in Microsoft Entra ID > Proprietà, salva ed esci in modo che questa elevazione non rimanga attiva.

Passaggio 5: configurare le autorizzazioni dell'API Microsoft Graph

Concedi le seguenti autorizzazioni API Microsoft Graph (tipo di applicazione) all'applicazione, quindi concedi il consenso dell'amministratore:

- `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
```

Passaggio 6: configura Azure Event Hub

AWS Config utilizza un Azure Event Hub per ricevere notifiche quasi in tempo reale sulle modifiche alla configurazione delle risorse nel tuo ambiente Azure. Lo script di configurazione crea l'infrastruttura Event Hub e la contrassegna per l'individuazione.

```
$ 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"
```

Dopo aver creato l'Event Hub, contrassegna il namespace per il rilevamento e assegna il ruolo di ricevitore dati:

```
$ 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**
>
> Nel formato tag`AWSConfig-account-id-region`, *`account-id`* è il tuo Account AWS ID a 12 cifre ed *`region`* è il Regione AWS luogo in cui stai creando il connettore (ad esempio,). `us-east-1` Questi valori identificano a quale regione Account AWS appartiene questa integrazione Event Hub.

Configurazione chiave:

- Namespace SKU: standard (obbligatorio per i gruppi di consumatori).
- Nome Event Hub —. `activitylog`
- Gruppo di consumatori —`AWSConfig`.
- Tag: `AWSConfig-`*`account-id-region`* con valore`activitylog`. Questo tag consente di AWS Config scoprire automaticamente l'Event Hub.
- Assegnazione dei ruoli: ricevitore dati di Azure Event Hub nel namespace.

Passaggio 7: configurazione del registro delle attività e dell'esportazione del registro di controllo Entra ID

Configura Azure per esportare i log delle attività e i registri di controllo di Entra ID nell'Event Hub.

Esportazione del registro delle attività:

Configura le impostazioni diagnostiche su ogni abbonamento per esportare i registri delle attività nell'Event Hub. Lo script di configurazione lo configura automaticamente per tutti gli abbonamenti monitorati. I registri delle attività registrano le attività a livello di abbonamento, comprese le assegnazioni di ruolo e le modifiche alle risorse.

Esportazione del registro di controllo Entra ID:

Configura le impostazioni diagnostiche su Microsoft Entra ID per esportare i registri di controllo nello stesso Event Hub. Accedere a Microsoft Entra ID > Monitoraggio > Impostazioni diagnostiche > Aggiungi impostazioni di diagnostica. Attivali AuditLogs e indirizzali al tuo Event Hub.

Esportazione continua di Microsoft Defender for Cloud (opzionale):

Per inoltrare gli avvisi di sicurezza di Defender for Cloud a Security Hub CSPM, configura l'esportazione continua nel tuo Event Hub. Nel portale di Azure, accedi a Microsoft Defender for Cloud > Impostazioni di ambiente > seleziona abbonamento > Esportazione continua. Seleziona Event Hub come destinazione di esportazione e scegli il tuo namespace Event Hub. Abilita gli avvisi di sicurezza come tipo di dati di esportazione.

Configurazione degli eventi relativi ai dati di Amazon Inspector (opzionale):

Se prevedi di utilizzare Amazon Inspector per la scansione di macchine virtuali di Azure, è necessaria una configurazione aggiuntiva degli eventi relativi ai dati. Per dettagli sulla configurazione degli eventi relativi Inspector-specific ai dati, consulta la documentazione di Amazon Inspector per l'integrazione con Azure.

Configurazione del Security Hub CSPM per l'integrazione con Microsoft Azure

Dopo aver completato le attività preliminari e configurato l'ambiente Microsoft Azure, puoi configurare AWS Security Hub CSPM per l'integrazione con Azure. Per configurare Security Hub CSPM per l'integrazione con Azure, devi creare un connettore. Dopo aver creato il connettore, si verificano i seguenti eventi:

1. Security Hub CSPM convalida le credenziali e la connettività di Azure all'ambiente Azure. Questo processo può richiedere alcuni minuti.
2. AWS Config inizia a scoprire e registrare i dati di configurazione per le risorse di Azure.
3. Security Hub CSPM inizia a generare risultati sulla gestione della postura per le risorse di Azure dopo il completamento della raccolta dei dati sulle risorse.

> **Note**
>
> Se hai già creato un connettore in Security Hub, un connettore collegato al servizio è stato creato automaticamente in Security Hub CSPM. Non è necessario creare un connettore separato gestito dal cliente a meno che non sia necessario un ambito diverso.

Argomenti

- Crea un connettore Azure
- Standard e controlli abilitanti
- Modifica l'ambito di un connettore Azure
- Verifica lo stato di integrità di un connettore di Azure
- Risolvi i problemi relativi a un connettore Azure
- In che modo Security Hub CSPM gestisce gli identificatori di risorse
- Controlli disponibili per Azure

Crea un connettore Azure

Per creare un connettore Microsoft Azure per il tuo ambiente, completa i passaggi seguenti utilizzando la console CSPM AWS di Security Hub o l'API.

1. Apri la console Security Hub CSPM.
2. Nel riquadro di navigazione, scegli Integrazioni.
3. Scegli Crea connettore Azure.
4. Per Azure Tenant ID, inserisci il tuo identificatore del tenant di Azure Active Directory.
5. Per Applicazione (ID client), inserisci l'ID dell'applicazione per la registrazione dell'app Azure che hai creato.
6. Configura impostazioni aggiuntive e l'ambito del connettore effettuando le seguenti operazioni:
    - In Nome, inserisci un nome univoco per il connettore. Il nome può contenere fino a 50 caratteri alfanumerici e può includere trattini (-).

> **Important**
>
> I nomi e le descrizioni vengono utilizzati per identificare i contenuti e ti consigliamo di non includere informazioni sensibili, riservate o di identificazione personale (PII).

- Per Descrizione, inserisci facoltativamente una breve descrizione del connettore. La descrizione può contenere fino a 200 caratteri.
- Per Abbonamenti, scegli Tutti gli abbonamenti per monitorare tutti gli abbonamenti attuali e futuri nel tenant o Abbonamenti specifici per monitorare solo gli abbonamenti specificati. Se scegli di monitorare solo abbonamenti specifici, inserisci l'ID per ognuno di essi.
- Per le regioni, scegli le aree di Azure in cui vengono distribuite le tue risorse.

> **Note**
>
> I controlli che valutano le risorse Microsoft Entra ID e Microsoft Graph richiedono che l'ambito globale dell'area sia incluso nella configurazione di integrazione. Se selezioni solo aree di Azure specifiche, questi controlli non genereranno risultati.

7. Rivedi la configurazione e scegli Crea connettore.

Dopo aver creato il connettore, Security Hub CSPM convalida le credenziali di Azure e inizia l'individuazione delle risorse. Il connettore dovrebbe mostrare lo stato Attivo entro 2-5 minuti.

Standard e controlli abilitanti

Dopo aver creato il connettore, devi abilitare gli standard di sicurezza di Azure per iniziare a generare risultati. Per informazioni generali sull'abilitazione degli standard e sulla gestione dei controlli, vedi Abilitazione degli standard e Abilitazione e disabilitazione dei controlli.

Standard disponibili

- CIS Microsoft Azure Foundations Benchmark v4.0 - Un benchmark di sicurezza ampiamente adottato che definisce le migliori pratiche per la protezione degli ambienti Azure. Ogni controllo valuta un aspetto specifico della configurazione di Azure (ad esempio, la crittografia degli account di archiviazione, le regole dei gruppi di sicurezza di rete, le impostazioni di identità e accesso).

- Best practice di Azure Foundational: valuta le risorse di Azure in base ai rischi di esposizione correlando gli indicatori di raggiungibilità della rete, accesso pubblico e dati sensibili. Genera risultati relativi al tipo di esposizione che evidenziano le risorse a rischio elevato.

Gli standard di Azure dispongono di un proprio set di controlli, separati dai controlli. AWS Non esistono controlli cross-cloud che valutino entrambe AWS le risorse di Azure in un unico controllo.

Abilitazione di uno standard

Puoi abilitare gli standard di Azure tramite la console CSPM di Security Hub o tramite. API/CLI Accedere a Standard nella console CSPM di Security Hub e abilitare lo standard desiderato. In alternativa, usa la CLI:

```
$ aws securityhub batch-enable-standards \
  --standards-subscription-requests '[{"StandardsArn": "Standard-ARN"}]' \
  --region your-aws-region
```

> **Note**
>
> Puoi abilitare gli standard di Azure prima o dopo la creazione del connettore: non sono accoppiati. Tuttavia, i risultati verranno generati solo dopo che sia il connettore che lo standard saranno attivi e i dati sulle risorse saranno stati raccolti.

Gestione dei controlli individuali

Una volta abilitato uno standard (in genere entro pochi secondi), puoi visualizzare e gestire i singoli controlli:

- Visualizza i controlli: utilizza la console Security Hub CSPM (Standard > seleziona standard > Controlli) o l'`list-standards-control-associations`API.
- Disattiva un controllo: se un controllo specifico non è applicabile al tuo ambiente, puoi disabilitarlo.
- Configura parametri personalizzati: alcuni controlli accettano parametri di input personalizzati (ad esempio, soglie di lunghezza delle password). Questi possono essere configurati tramite l'`update-security-control`API.

Note importanti

- Gli standard di Azure si applicano in modo uniforme all'intero ambito dei connettori. Non puoi abilitare standard o controlli diversi per sottoscrizioni di Azure diverse all'interno dello stesso connettore.
- I controlli dipendono dalla disponibilità dei dati delle risorse. Ogni controllo valuta un tipo di risorsa di Azure specifico. Se non AWS Config ha ancora raccolto i dati di configurazione per un particolare tipo di risorsa, il controllo genererà una ricerca PASS predefinita per tali risorse. Questi risultati PASS predefiniti verranno aggiornati automaticamente con valutazioni accurate non appena arrivano i dati sulle risorse. Non considerate accurati i punteggi iniziali di conformità fino al completamento della raccolta dei dati sulle risorse.
- I parametri di input personalizzati per i controlli di sicurezza possono essere configurati anche prima di creare un connettore: persistono indipendentemente.
- I controlli che valutano le impostazioni a livello di abbonamento (ad esempio, piani Microsoft Defender, avvisi del registro delle attività) producono un risultato per sottoscrizione di Azure anziché per singola risorsa.
- Gli standard multicloud non possono essere inclusi nelle politiche di configurazione centrale. È necessario gestire l'abilitazione standard di Azure in modo indipendente in ogni e. Account AWS Regione AWS

Modifica l'ambito di un connettore Azure

Dopo aver creato un connettore Microsoft Azure, puoi modificare l'ambito del connettore modificando le sottoscrizioni di Azure o le aree di Azure che monitora. Se modifichi l'ambito, la maggior parte dei tipi di modifiche avrà effetto entro circa 15 minuti.

Prima di regolare l'ambito, tenete presente quanto segue:

- L'ambito di un connettore gestito dal cliente non può superare l'ambito di qualsiasi connettore collegato al servizio esistente nello stesso account e nella stessa regione.
- Quando si amplia l'ambito, Security Hub CSPM inizia a generare risultati per nuove risorse dopo aver AWS Config raccolto i relativi dati di configurazione.
- Quando si riduce l'ambito, i risultati esistenti relativi alle risorse rimosse passano allo stato di archiviazione.

Verifica lo stato di integrità di un connettore di Azure

Puoi controllare lo stato di un connettore Microsoft Azure in qualsiasi momento. Vai a Integrazioni nella console CSPM di Security Hub e conferma che il connettore mostri lo stato Attivo.

I risultati iniziali vengono in genere visualizzati entro 15-30 minuti dal completamento della raccolta dei dati sulle risorse.

> **Note**
>
> Lo stato di salute del connettore alla fine è costante. Quando si verifica un problema di autorizzazione o configurazione, lo stato del connettore passa rapidamente a Degradato con un messaggio utilizzabile. Tuttavia, dopo aver risolto il problema, lo stato può richiedere fino a 24 ore per tornare a Connesso.
>
> - Uno stato Degrado dopo una correzione recente non indica necessariamente la presenza di un problema in corso.
> - Per una visibilità in tempo reale degli errori di registrazione, controlla le CloudWatch metriche nel namespace.

Risolvi i problemi relativi a un connettore Azure

In caso di problemi con il connettore, utilizza le seguenti informazioni per diagnosticare e risolvere i problemi più comuni.

Lo stato del connettore non è integro

Questo problema si verifica in genere se le credenziali federate non sono configurate correttamente in Azure.

Per risolvere questo problema, verifica che l'URL dell'emittente del token e l'ARN dell'oggetto nelle credenziali federate di Azure corrispondano ai tuoi. Account AWS

Nessun risultato dopo 30 minuti

Questo problema può verificarsi se Event Hub non riceve i registri delle attività o se non è abilitato alcuno standard.

Per risolvere questo problema, verifica che lo spazio dei nomi di Event Hub sia etichettato correttamente (`AWSConfig-`*`account-id`*`-`*`region`*`=activitylog`), che il gruppo di

`AWSConfig` consumatori esista, che il ruolo Data Receiver sia assegnato e che almeno uno standard di Azure sia abilitato.

Impossibile registrare alcune risorse di Azure

L'errore può verificarsi per uno dei seguenti motivi:

- L'ambiente Azure non soddisfa i prerequisiti per la registrazione delle risorse.
- La registrazione dell'app non dispone del consenso dell'amministratore per le autorizzazioni dell'API Microsoft Graph.
- L'assegnazione del ruolo Reader non copre tutti gli ambiti richiesti.
- Il tenant Microsoft Entra ID non dispone dei dati di registro richiesti.

Per risolvere l'errore, procedi come segue:

1. Per confermare che l'ambiente soddisfa tutti i requisiti, consulta Prerequisiti per Microsoft Azure.
2. Verifica che la registrazione dell'app disponga delle autorizzazioni necessarie per l'API Microsoft Graph con il consenso dell'amministratore.
3. Verifica che il responsabile del servizio abbia il ruolo di lettore nell'ambito del gruppo di gestione principale del tenant.

Il connettore rimane nello stato In sospeso

Questo problema può verificarsi se la registrazione dell'app Azure non è configurata correttamente.

Per risolvere questo problema, verifica che l'URL dell'emittente delle credenziali di identità federata e l'identificatore del soggetto corrispondano ai tuoi. Account AWS Verifica inoltre che sia stato concesso il consenso dell'amministratore per tutte le autorizzazioni necessarie per l'API Microsoft Graph.

In che modo Security Hub CSPM gestisce gli identificatori di risorse

Abilitando l'integrazione di Azure per AWS Security Hub CSPM, gli identificatori di risorse di altri provider cloud verranno archiviati in AWS Security AWS Config Hub CSPM e altri AWS servizi (se necessario) come metadati relativi alla gestione dei dati di configurazione delle risorse corrispondenti raccolti dagli altri provider cloud. Tali identificatori di risorse non costituiscono i Contenuti dell'utente e consigliamo di non includere in essi informazioni sensibili, riservate o di identificazione personale.

I seguenti identificatori dell'ambiente cloud connesso vengono archiviati e utilizzati da per fornire funzionalità di sicurezza AWS multicloud:

- Identificatori di risorse: Azure Tenant ID, ID di sottoscrizione, posizione (regione), ID risorsa (ID o nomi dei gruppi di risorse, provider di risorse, tipo di risorsa)

Le relazioni tra questi identificatori, incluso il modo in cui le risorse si relazionano tra loro e il modo in cui i risultati si relazionano alle risorse, vengono archiviate anche come metadati di servizio. AWS utilizza questi identificatori per la correlazione delle risorse, l'associazione dei risultati alle risorse, la registrazione operativa del servizio e la deduplicazione.

Controlli disponibili per Azure

Dopo aver abilitato gli standard di Azure, i seguenti 122 controlli valutano le tue risorse di Azure. I controlli sono distribuiti su due standard:

- CIS Microsoft Azure Foundations Benchmark v4.0 — 96 controlli mappati su sezioni CIS specifiche
- Azure Foundational Best Practices: 26 controlli che coprono procedure consigliate di sicurezza aggiuntive

> **Note**
>
> I controlli che valutano le risorse Microsoft Entra ID e Microsoft Graph richiedono che l'ambito globale dell'area sia incluso nella configurazione di integrazione.

Controlli di Azure disponibili

Titolo di controllo	Tipo di risorsa	Standard
Le app Azure Container con identità gestita abilitata devono seguire il privilegio minimo	`microsoft.app/containerapps`	Procedure consigliate di base per Azure
Le app contenitore di Azure non devono passare le credenziali di Azure SDK come variabili di ambiente	`microsoft.app/containerapps`	Procedure consigliate di base per Azure

Titolo di controllo	Tipo di risorsa	Standard
Le app contenitore di Azure non devono avere l'ingresso esterno abilitato	`microsoft.app/containerapps`	Procedure consigliate di base per Azure
Gli ambienti delle app Azure Container non devono avere accesso NSG illimitato	`microsoft.app/containerapps`	Procedure consigliate di base di Azure
Gli ambienti gestiti dell'app Azure Container non devono avere l'IP pubblico abilitato	`microsoft.app/managedenvironments`	Procedure consigliate di base di Azure
Le assegnazioni di ruolo di Azure non devono garantire un ampio accesso amministrativo nell'ambito della sottoscrizione	`microsoft.authorization/roleassignments`	Best practice di base di Azure
Le assegnazioni di ruolo di Azure non devono concedere il ruolo User Access Administrator	`microsoft.authorization/roleassignments`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le definizioni dei ruoli personalizzati di Azure non devono avere autorizzazioni amministrative wildcard	`microsoft.authorization/roledefinitions`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le assegnazioni delle policy di Microsoft Cloud Security Benchmark devono avere la modalità di applicazione abilitata	`microsoft.authorization/policyassignments`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I cluster Azure Kubernetes Service (AKS) non devono avere server API accessibili pubblicamente senza restrizioni IP	`microsoft.containerservice/managedclusters`	Procedure consigliate di base per Azure

Titolo di controllo	Tipo di risorsa	Standard
I cluster Azure Kubernetes Service (AKS) devono crittografare i segreti di Kubernetes quando sono inattivi	`microsoft.containerservice/managedclusters`	Procedure consigliate di base per Azure
I cluster Azure Kubernetes Service (AKS) devono eseguire una versione di Kubernetes supportata	`microsoft.containerservice/managedclusters`	Procedure consigliate di base per Azure
Gli account di Azure Cosmos DB devono avere il backup continuo abilitato	`microsoft.documentdb/databaseaccounts`	Procedure consigliate di base di Azure
I server flessibili di Azure Database per MySQL devono avere l'accesso alla rete pubblica disabilitato	`microsoft.dbformysql/flexibleservers`	Procedure consigliate di base per Azure
Le aree di lavoro di Azure Databricks devono essere distribuite in una rete virtuale gestita dal cliente	`microsoft.databricks/workspaces`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le aree di lavoro di Azure Databricks devono avere configurata la consegna dei log diagnostici	`microsoft.databricks/workspaces`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le aree di lavoro di Azure Databricks devono usare chiavi gestite dal cliente per la crittografia gestita del disco	`microsoft.databricks/workspaces`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le politiche di autorizzazione degli ID Microsoft Entra dovrebbero vietare agli utenti predefiniti di registrare le applicazioni	`microsoft.graph/policies/authorizationpolicy`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
L'ID Azure Entra dovrebbe avere le impostazioni di sicurezza predefinite abilitate	`microsoft.graph/policies/identitysecuritydefaultsenforcementpolicy`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I tenant di Microsoft Entra devono disporre di una politica di accesso condizionale che blocchi l'accesso da località geografiche non consentite	`microsoft.graph/organization`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I tenant di Microsoft Entra devono disporre di una politica di accesso condizionale che blocchi il flusso di autenticazione del codice del dispositivo	`microsoft.graph/organization`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le policy di accesso condizionale di Azure dovrebbero richiedere l'autenti cazione a più fattori per tutti gli utenti	`microsoft.graph/organization`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I tenant di Microsoft Entra devono richiedere l'autenticazione a più fattori per gli accessi rischiosi tramite una politica di accesso condizionale	`microsoft.graph/organization`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I tenant di Azure devono richiedere l'autenticazione a più fattori tramite l'accesso condizionale per l'API di gestione dei servizi di Azure	`microsoft.graph/organization`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Almeno una politica di accesso condizion ale deve richiedere l'autenticazione a più fattori per Microsoft Admin Portals	`microsoft.graph/organization`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
Le politiche di autorizzazione di Microsoft Entra dovrebbero impedire agli utenti non amministratori di creare tenant	`microsoft.graph/policies/authorizationpolicy`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I criteri dei metodi di autenticazione ID Microsoft Entra devono impostare il periodo di riconferma su un valore diverso da zero	`microsoft.graph/policies/authenticationmethodspolicy`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I criteri di autorizzazione di Microsoft Entra dovrebbero limitare il consenso degli utenti per le applicazioni	`microsoft.graph/policies/authorizationpolicy`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le politiche di autorizzazione di Azure dovrebbero limitare il consenso degli utenti alle app per editori verificate	`microsoft.graph/policies/authorizationpolicy`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le politiche di autorizzazione di Microsoft Entra devono limitare l'accesso degli utenti guest ai propri oggetti di directory.	`microsoft.graph/policies/authorizationpolicy`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le politiche di autorizzazione di Azure dovrebbero limitare gli inviti degli ospiti solo ai ruoli di amministratore	`microsoft.graph/policies/authorizationpolicy`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le politiche di autorizzazione di Azure dovrebbero limitare la creazione di gruppi di sicurezza agli amministratori	`microsoft.graph/policies/authorizationpolicy`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
I tenant di Microsoft Entra devono richiedere l'autenticazione a più fattori per registrare o unire i dispositivi	`microsoft.graph/organization`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I ruoli della directory ID Microsoft Entra devono avere da 2 a 4 amministratori globali	`microsoft.graph/directoryrole`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le impostazioni del gruppo Azure Entra ID devono limitare la creazione di gruppi agli amministratori	`microsoft.graph/organization`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere un'impostazione diagnostica configurata per i log delle attività	`microsoft.insights/diagnosticsettings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere un avviso di registro delle attività per la creazione dell'assegnazione delle policy	`microsoft.insights/activitylogalerts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere un avviso del registro delle attività per l'eliminazione dell'assegnazione delle policy	`microsoft.insights/activitylogalerts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere un avviso di registro delle attività per la creazione o l'aggiornamento delle operazioni del Network Security Group	`microsoft.insights/activitylogalerts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
Le sottoscrizioni di Azure devono avere un avviso del registro delle attività per l'eliminazione del Network Security Group	`microsoft.insights/activitylogalerts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere un avviso del registro delle attività per la creazione o l'aggiornamento della soluzione di sicurezza	`microsoft.insights/activitylogalerts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere un avviso del registro delle attività per l'eliminazione di Security Solution	`microsoft.insights/activitylogalerts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere un avviso del registro delle attività per la creazione o l'aggiornamento delle regole del firewall di SQL Server	`microsoft.insights/activitylogalerts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere un avviso del registro delle attività per l'eliminazione delle regole del firewall di SQL Server	`microsoft.insights/activitylogalerts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere un avviso del registro delle attività configurato per le operazioni di creazione o aggiornamento di indirizzi IP pubblici	`microsoft.insights/activitylogalerts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere un avviso del registro delle attività per l'eliminazione degli indirizzi IP pubblici	`microsoft.insights/activitylogalerts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
Le sottoscrizioni di Azure devono avere un avviso del registro delle attività per gli incidenti di Service Health	`microsoft.insights/activitylogalerts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere almeno un componente Application Insights configurato	`microsoft.insights/components`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Azure Key Vaults dovrebbe avere la protezione soft delete e purge abilitata	`microsoft.keyvault/vaults`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Azure Key Vaults dovrebbe avere il controllo degli accessi basato sui ruoli abilitato	`microsoft.keyvault/vaults`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Azure Key Vaults dovrebbe avere l'accesso alla rete pubblica disabilitato quando si usano endpoint privati	`microsoft.keyvault/vaults`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Azure Key Vaults deve usare endpoint privati	`microsoft.keyvault/vaults`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Azure Key Vaults dovrebbe avere la protezione da eliminazione abilitata	`microsoft.keyvault/vaults`	Procedure consigliate di base di Azure
Azure Key Vaults dovrebbe limitare l'accesso alla rete	`microsoft.keyvault/vaults`	Procedure consigliate di base per Azure

Titolo di controllo	Tipo di risorsa	Standard
Azure Key Vaults dovrebbe avere la registrazione abilitata AuditEvent	`microsoft.keyvault/vaults`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le chiavi di Azure Key Vault negli archivi RBAC devono avere una data di scadenza impostata	`microsoft.keyvault/vaults/keys`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le chiavi di Azure Key Vault negli archivi non RBAC devono avere una data di scadenza impostata	`microsoft.keyvault/vaults/keys`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I segreti di Azure Key Vault nei vault devono avere una data di scadenza RBAC-enabled impostata	`microsoft.keyvault/vaults/secrets`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I segreti di Azure Key Vault negli archivi non RBAC devono avere una data di scadenza impostata	`microsoft.keyvault/vaults/secrets`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le chiavi di Azure Key Vault devono avere la rotazione automatica abilitata	`microsoft.keyvault/vaults/keys`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I gruppi di sicurezza di rete di Azure devono limitare l'accesso RDP in entrata da Internet	`microsoft.network/networksecuritygroups`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
I gruppi di sicurezza di rete di Azure devono limitare l'accesso UDP in entrata da Internet	`microsoft.network/networksecuritygroups`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I gruppi di sicurezza di rete di Azure devono limitare l'accesso HTTP in entrata da Internet	`microsoft.network/networksecuritygroups`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoreti di Azure Application Gateway non devono avere accesso NSG illimitato	`microsoft.network/networksecuritygroups`	Procedure consigliate di base per Azure
I gruppi di sicurezza di rete di Azure devono avere una regola deny-all esplicita	`microsoft.network/networksecuritygroups`	Procedure consigliate di base per Azure
I gruppi di sicurezza di rete di Azure non dovrebbero consentire l'accesso in entrata illimitato a porte con restrizioni	`microsoft.network/networksecuritygroups`	Procedure consigliate di base per Azure
I log di flusso di Azure Network Watcher devono avere la registrazione del flusso di rete virtuale abilitata con l'analisi del traffico inviata a Log Analytics	`microsoft.network/networkwatchers/flowlogs`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I gruppi di sicurezza di rete di Azure devono limitare l'accesso SSH da Internet	`microsoft.network/networksecuritygroups`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere almeno un host Azure Bastion	`microsoft.network/bastionhosts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
Le sottoscrizioni di Azure devono avere Microsoft Defender for Servers abilitato	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le macchine devono disporre di una valida soluzione di valutazione delle vulnerabilità implementata in Microsoft Defender for Cloud	`microsoft.security/assessments`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere l'integrazione della protezione degli endpoint con Microsoft Defender for Cloud abilitata	`microsoft.security/settings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere la scansione senza agente per le macchine abilitata in Microsoft Defender for Servers	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere il File Integrity Monitoring abilitato in Defender for Servers	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
La sottoscrizione di Azure deve avere Microsoft Defender for Containers abilitato	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere Microsoft Defender for Storage abilitato	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
Le sottoscrizioni di Azure devono avere Microsoft Defender for App Service abilitato	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere Microsoft Defender for Azure Cosmos DB abilitato	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere Microsoft Defender per database relazionali open source abilitato	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere Microsoft Defender for Azure SQL Databases abilitato	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere Microsoft Defender for SQL Servers on Machines abilitato	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere Microsoft Defender for Key Vault abilitato	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere Microsoft Defender for Resource Manager abilitato	`microsoft.security/pricings`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
Le valutazioni degli aggiornamenti di sistema sulle macchine virtuali dovrebbero essere segnalate come corrette da Microsoft Defender for Cloud	`microsoft.security/assessments`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I contatti di sicurezza di Microsoft Defender for Cloud devono notificare il ruolo di Proprietario degli avvisi	`microsoft.security/securitycontacts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I contatti di sicurezza di Microsoft Defender for Cloud devono avere un indirizzo e-mail aggiuntivo configurato	`microsoft.security/securitycontacts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I contatti di sicurezza di Azure devono avere le notifiche e-mail di avviso abilitate con una severità minima sufficientemente inclusiva	`microsoft.security/securitycontacts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I contatti di sicurezza di Azure devono avere le notifiche e-mail relative ai percorsi di attacco abilitate con un livello di rischio configurato	`microsoft.security/securitycontacts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le sottoscrizioni di Azure devono avere Microsoft Defender for IoT abilitato	`microsoft.security/iotsecuritysolutions`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I server SQL di Azure devono avere l'accesso alla rete pubblica disabilitato	`microsoft.sql/servers`	Procedure consigliate di base per Azure
I server SQL devono avere un amministratore di Azure Active Directory configurato	`microsoft.sql/servers`	Procedure consigliate di base di Azure

Titolo di controllo	Tipo di risorsa	Standard
I database SQL di Azure devono avere il backup georidondante abilitato	`microsoft.sql/servers/databases`	Procedure consigliate di base per Azure
I server SQL di Azure non devono usare nomi di account amministratore predefiniti	`microsoft.sql/servers`	Best practice di base di Azure
L'aggiornamento automatico della versione secondaria delle istanze gestite di Azure SQL dovrebbe essere abilitato	`microsoft.sql/managedinstances`	Procedure consigliate di base per Azure
Gli account di archiviazione di Azure devono usare chiavi gestite dal cliente per la crittografia	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I servizi di gestione dei file degli account di archiviazione di Azure devono avere l'opzione soft delete abilitata per le condivisioni di file	`microsoft.storage/storageaccounts/fileservices`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le condivisioni di file degli account di archiviazione di Azure devono limitare le versioni del protocollo SMB a SMB 3.1.1	`microsoft.storage/storageaccounts/fileservices`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono usare un algoritmo di crittografia del canale SMB sicuro per le condivisioni di file	`microsoft.storage/storageaccounts/fileservices`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono avere un promemoria di rotazione delle chiavi configurato	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
Gli account di archiviazione di Azure dovrebbero avere l'accesso con chiave condivisa disabilitato	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono utilizzare endpoint privati per l'accesso	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono avere l'accesso alla rete pubblica disabilitato	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono avere l'accesso alla rete predefinito impostato su Negare	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Per impostazione predefinita, gli account di archiviazione devono utilizzare l'autorizzazione Microsoft Entra nel portale di Azure	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono richiedere un trasferimento sicuro	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono consentire ai servizi di Azure affidabili di aggirare le regole di rete	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
Gli account di archiviazione di Azure devono essere configurati con la versione TLS minima richiesta	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono avere la replica tra tenant disabilitata	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono avere l'accesso anonimo ai BLOB disabilitati	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono limitare l'eliminazione permanente dei blob	`microsoft.storage/storageaccounts/blobservices`	Procedure consigliate di base per Azure
Gli account di archiviazione di Azure contenenti i log delle attività devono essere crittografati con una chiave gestita dal cliente	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I servizi blob dell'account di archiviazione di Azure devono avere blob soft delete abilitato	`microsoft.storage/storageaccounts/blobservices`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
I servizi blob dell'account di archiviazione di Azure devono avere il controllo delle versioni abilitato	`microsoft.storage/storageaccounts/blobservices`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Titolo di controllo	Tipo di risorsa	Standard
I servizi blob dell'account di archiviazione di Azure devono avere blob e container soft delete abilitati	`microsoft.storage/storageaccounts/blobservices`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Agli account di archiviazione di Azure deve essere applicato un blocco di eliminazione di Azure Resource Manager	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono avere un blocco di gestione delle risorse ReadOnly	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Gli account di archiviazione di Azure devono usare l'archiviazione geo-ridondante	`microsoft.storage/storageaccounts`	Benchmark CIS per Microsoft Azure Foundations versione 4.0
Le app Azure Function devono limitare l'accesso amministrativo	`microsoft.web/sites/config`	Best practice di base di Azure
Le funzioni di Azure non dovrebbero consentire la chiamata anonima di trigger HTTP	`microsoft.web/sites/functions`	Procedure consigliate di base di Azure
Le app Web e le app funzionali del Servizio app di Azure non devono usare versioni di runtime non supportate	`microsoft.web/sites`	Best practice di base di Azure
Le app Azure Function con piani Premium o Dedicato devono essere integrate con una rete virtuale	`microsoft.web/sites`	Procedure consigliate di base per Azure

Titolo di controllo	Tipo di risorsa	Standard
Le app Web del Servizio app di Azure devono avere i log HTTP abilitati nelle impostazioni di diagnostica	`microsoft.web/sites`	Benchmark CIS per Microsoft Azure Foundations versione 4.0

Eliminazione di un connettore Microsoft Azure in Security Hub CSPM

Dopo aver creato un connettore Microsoft Azure in AWS Security Hub CSPM, puoi eliminarlo in qualsiasi momento. Se elimini un connettore, Security Hub CSPM interrompe l'esecuzione dei controlli di gestione della postura e del monitoraggio delle vulnerabilità per il tuo ambiente Azure. Security Hub CSPM smette inoltre di generare nuove informazioni sull'ambiente in uso. I risultati esistenti vengono conservati per 90 giorni. L'inventario delle risorse rimane com'era quando il connettore è stato eliminato e viene rimosso dopo 90 giorni.

Quando elimini un connettore, tieni presente quanto segue:

- Security Hub CSPM non elimina la registrazione delle applicazioni Azure e l'infrastruttura Event Hub nell'ambiente Azure. È necessario eliminarli manualmente, direttamente in Microsoft Azure. Per sapere come, vedi Rimuovere un'applicazione nella documentazione di Microsoft Azure.
- Se il connettore è un connettore gestito dal cliente ed esiste anche un connettore collegato al servizio, l'eliminazione del connettore gestito dal cliente non influisce sul connettore collegato al servizio. Security Hub CSPM continua a ricevere risultati sulla gestione della postura tramite il connettore collegato al servizio.
- I risultati esistenti passano allo stato di archiviazione entro 3-5 giorni e vengono eliminati dopo il periodo di conservazione di 90 giorni.

Per eliminare un connettore Azure

1. Apri la console Security Hub CSPM.
2. Nel riquadro di navigazione, scegli Integrazioni.
3. Seleziona il tuo connettore.
4. Scegli Elimina.
5. Quando richiesto, conferma che desideri eliminare il connettore.

Dopo l'eliminazione, puoi facoltativamente pulire le risorse di Azure create durante la configurazione:

- Elimina la registrazione dell'app in Microsoft Entra ID.
- Elimina lo spazio dei nomi e il gruppo di risorse di Event Hub.
- Rimuovi le impostazioni diagnostiche che esportano i registri delle attività e i registri di controllo Entra ID.

Creazione e aggiornamento dei risultati in Security Hub CSPM

In AWS Security Hub CSPM, un risultato è una registrazione osservabile di un controllo di sicurezza o di un rilevamento relativo alla sicurezza. Un risultato può provenire da una delle seguenti fonti:

- Un controllo di sicurezza per un controllo in Security Hub CSPM.
- Un'integrazione con un'altra. Servizio AWS
- Un'integrazione con un prodotto di terze parti.
- Un'integrazione personalizzata.

Security Hub CSPM normalizza i risultati provenienti da tutte le fonti in una sintassi e un formato standard chiamati AWS Security Finding Format (ASFF). Per informazioni dettagliate su questo formato, incluse le descrizioni dei singoli campi ASFF, vedere. AWS Formato ASFF (Security Finding Format) Se abiliti l'aggregazione tra regioni, Security Hub CSPM aggrega automaticamente anche i risultati nuovi e aggiornati da tutte le regioni collegate a un'area di aggregazione specificata. Per ulteriori informazioni, consulta Comprendere l'aggregazione interregionale in Security Hub CSPM.

Dopo aver creato un risultato, può essere aggiornato come segue:

- Un provider di ricerca può utilizzare il BatchImportFindingsfunzionamento dell'API CSPM Security Hub per aggiornare le informazioni generali sul risultato. I provider di risultati possono aggiornare solo i risultati che hanno creato.
- Un cliente può utilizzare la console CSPM di Security Hub o il BatchUpdateFindingsfunzionamento dell'API CSPM di Security Hub per aggiornare lo stato dell'indagine sulla scoperta. L'`BatchUpdateFindings`operazione può essere utilizzata anche da uno strumento SIEM, di ticketing, di gestione degli incidenti, SOAR o altro tipo di strumento per conto di un cliente.

Per ridurre il rumore dei risultati e semplificare il tracciamento e l'analisi dei singoli risultati, Security Hub CSPM elimina automaticamente i risultati che non sono stati aggiornati di recente. La tempistica

con cui Security Hub CSPM esegue questa operazione dipende dal fatto che un risultato sia attivo o archiviato:

- Un risultato attivo è un risultato il cui stato record () è. `RecordState` `ACTIVE` Security Hub CSPM archivia i risultati attivi per 90 giorni. Se un risultato attivo non viene aggiornato per 90 giorni, scade e Security Hub CSPM lo elimina definitivamente.
- Un risultato archiviato è un risultato il cui stato record () è. `RecordState` `ARCHIVED` Security Hub CSPM archivia i risultati archiviati per 30 giorni. Se un risultato archiviato non viene aggiornato per 30 giorni, scade e Security Hub CSPM lo elimina definitivamente.

Per i risultati del controllo, ovvero i risultati generati da Security Hub CSPM dai controlli di sicurezza per i controlli, Security Hub CSPM determina se un risultato è scaduto in base al valore del campo del risultato. `UpdatedAt` Se questo valore risale a più di 90 giorni fa per un risultato attivo, Security Hub CSPM elimina definitivamente il risultato. Se questo valore risale a più di 30 giorni fa per un risultato archiviato, Security Hub CSPM elimina definitivamente il risultato.

Per tutti gli altri tipi di risultati, Security Hub CSPM determina se un risultato è scaduto in base ai valori per i `UpdatedAt` campi `ProcessedAt` e del risultato. Security Hub CSPM confronta i valori di questi campi e determina quale è più recente. Se il valore più recente risale a più di 90 giorni fa per un risultato attivo, Security Hub CSPM elimina definitivamente il risultato. Se il valore più recente risale a più di 30 giorni fa per un risultato archiviato, Security Hub CSPM elimina definitivamente il risultato. I provider di ricerca possono modificare il valore per il `UpdatedAt` campo di uno o più risultati utilizzando il BatchImportFindingsfunzionamento dell'API CSPM Security Hub.

Per conservare i risultati a lungo termine, puoi esportarli in un bucket S3. Puoi farlo utilizzando un'azione personalizzata con una EventBridge regola Amazon. Per ulteriori informazioni, consulta Utilizzo EventBridge per la risposta e la correzione automatiche.

Argomenti

- BatchImportFindings per trovare fornitori
- BatchUpdateFindings per i clienti
- Revisione dei dettagli e della cronologia dei risultati in Security Hub CSPM
- Filtraggio dei risultati in Security Hub CSPM
- Raggruppamento dei risultati in Security Hub CSPM
- Impostazione dello stato del flusso di lavoro dei risultati in Security Hub CSPM
- Invio dei risultati a un'azione CSPM personalizzata di Security Hub

- AWS Formato ASFF (Security Finding Format)

BatchImportFindings per trovare fornitori

I provider di ricerca possono utilizzare l'BatchImportFindingsoperazione per creare nuovi risultati in AWS Security Hub CSPM. Possono utilizzare questa operazione anche per aggiornare i risultati che hanno creato. I fornitori di servizi di ricerca non possono aggiornare i risultati che non hanno creato.

I clienti, i SIEM, il ticketing, il SOAR e altri tipi di strumenti devono utilizzare l'BatchUpdateFindingsoperazione per apportare aggiornamenti relativi all'analisi dei risultati ottenuti dai fornitori di servizi di ricerca. Per ulteriori informazioni, consulta the section called "BatchUpdateFindings per i clienti".

Quando Security Hub CSPM riceve una `BatchImportFindings` richiesta per creare o aggiornare un risultato, genera automaticamente un Security Hub Findings - Importedevento in Amazon. EventBridge Puoi intraprendere azioni automatiche su quell'evento. Per ulteriori informazioni, consulta the section called "Risposta e riparazione automatiche".

Prerequisiti per l'utilizzo di **`BatchImportFindings`**

`BatchImportFindings`deve essere chiamato da uno dei seguenti:

- L'account associato ai risultati. L'identificatore dell'account associato deve corrispondere al valore dell'`AwsAccountId`attributo per il risultato.
- Un account consentito nell'elenco dei partner CSPM ufficiali di Security Hub.

Security Hub CSPM può accettare la ricerca di aggiornamenti solo per gli account con Security Hub CSPM abilitato. Anche il provider di risultati deve essere abilitato. Se Security Hub CSPM è disabilitato o l'integrazione del provider di ricerca non è abilitata, i risultati vengono restituiti nell'`FailedFindings`elenco, con un `InvalidAccess` errore.

Determinazione per creare o aggiornare un risultato

Per determinare se creare o aggiornare un risultato, Security Hub CSPM controlla il `ID` campo. Se il valore di `ID` non corrisponde a un risultato esistente, Security Hub CSPM crea un nuovo risultato.

Se `ID` corrisponde a un risultato esistente, Security Hub CSPM controlla il `UpdatedAt` campo per l'aggiornamento e procede come segue:

- Se `UpdatedAt` l'aggiornamento corrisponde o si verifica prima `UpdatedAt` del risultato esistente, Security Hub CSPM ignora la richiesta di aggiornamento.
- Se `UpdatedAt` l'aggiornamento avviene dopo `UpdatedAt` il risultato esistente, Security Hub CSPM aggiorna il risultato esistente.

Restrizioni sulla ricerca di aggiornamenti con **`BatchImportFindings`**

I fornitori di servizi di ricerca non possono `BatchImportFindings` utilizzare per aggiornare i seguenti attributi di un risultato esistente:

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Security Hub CSPM ignora qualsiasi contenuto fornito in una `BatchImportFindings` richiesta per questi attributi. I clienti o le entità che agiscono per loro conto (come gli strumenti di ticketing) possono utilizzare `BatchUpdateFindings` per aggiornare questi attributi.

Aggiornamento dei risultati con FindingProviderFields

Inoltre, i fornitori di servizi di ricerca non dovrebbero `BatchImportFindings` aggiornare i seguenti attributi di primo livello nel AWS Security Finding Format (ASFF):

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Invece, i provider di ricerca dovrebbero utilizzare l'`FindingProviderFields`oggetto per fornire valori per questi attributi.

Esempio

```
"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" ]
}
```

Per `BatchImportFindings` le richieste, Security Hub CSPM gestisce i valori negli attributi di primo livello e nel `FindingProviderFields`modo seguente.

(Preferito) **`BatchImportFindings`** fornisce un valore per un attributo in **`FindingProviderFields`**, ma non fornisce un valore per l'attributo di primo livello corrispondente.

Ad esempio`FindingProviderFields.Confidence`, `BatchImportFindings` fornisce ma non fornisce`Confidence`. Questa è l'opzione preferita per `BatchImportFindings` le richieste.

Security Hub CSPM aggiorna il valore dell'attributo in. `FindingProviderFields`

Replica il valore nell'attributo di primo livello solo se l'attributo non è già stato aggiornato da. `BatchUpdateFindings`

`BatchImportFindings`fornisce un valore per un attributo di primo livello, ma non fornisce un valore per l'attributo corrispondente in. **`FindingProviderFields`**

Ad esempio`Confidence`, `BatchImportFindings` fornisce ma non fornisce`FindingProviderFields.Confidence`.

Security Hub CSPM utilizza il valore per aggiornare l'attributo in. `FindingProviderFields` Sovrascrive qualsiasi valore esistente.

Security Hub CSPM aggiorna l'attributo di primo livello solo se l'attributo non è già stato aggiornato da. `BatchUpdateFindings`

`BatchImportFindings`fornisce un valore sia per un attributo di primo livello che per l'attributo corrispondente in. **`FindingProviderFields`**

Ad esempio, `BatchImportFindings` fornisce `Confidence` sia`FindingProviderFields.Confidence`.

Per una nuova scoperta, Security Hub CSPM utilizza il valore in `FindingProviderFields` per compilare sia l'attributo di primo livello che l'attributo corrispondente in. `FindingProviderFields` Non utilizza il valore dell'attributo di primo livello fornito.

Per un risultato esistente, Security Hub CSPM utilizza entrambi i valori. Tuttavia, aggiorna il valore dell'attributo di primo livello solo se l'attributo non è già stato aggiornato da. `BatchUpdateFindings`

BatchUpdateFindings per i clienti

AWS I clienti di Security Hub CSPM e le entità che agiscono per loro conto possono utilizzare l'BatchUpdateFindingsoperazione per aggiornare le informazioni relative all'elaborazione dei risultati CSPM di Security Hub rilevati dai provider di ricerca. In qualità di cliente, puoi utilizzare direttamente questa operazione. Anche gli strumenti SIEM, di ticketing, di gestione degli incidenti e SOAR possono utilizzare questa operazione per conto di un cliente.

Non è possibile utilizzare l'`BatchUpdateFindings`operazione per creare nuove scoperte. Tuttavia, puoi utilizzarla per aggiornare fino a 100 risultati esistenti alla volta. In una `BatchUpdateFindings` richiesta, specificate quali risultati aggiornare, quali campi del AWS Security Finding Format (ASFF) aggiornare per i risultati e i nuovi valori per i campi. Security Hub CSPM aggiorna quindi i risultati come specificato nella richiesta. Questo processo può richiedere alcuni minuti. Se aggiorni i risultati utilizzando l'`BatchUpdateFindings`operazione, gli aggiornamenti non influiscono sui valori esistenti per il `UpdatedAt` campo dei risultati.

Quando Security Hub CSPM riceve una `BatchUpdateFindings` richiesta di aggiornamento di un risultato, genera automaticamente un Security Hub Findings – Importedevento in Amazon. EventBridge Facoltativamente, puoi utilizzare questo evento per intraprendere azioni automatiche sul risultato specificato. Per ulteriori informazioni, consulta the section called "Risposta e riparazione automatiche".

Campi disponibili per BatchUpdateFindings

Se hai effettuato l'accesso a un account amministratore CSPM di Security Hub, puoi utilizzarlo `BatchUpdateFindings` per aggiornare i risultati generati dall'account amministratore o dagli account dei membri. Gli account dei membri possono essere utilizzati `BatchUpdateFindings` per aggiornare i risultati solo per il proprio account.

I clienti possono utilizzare `BatchUpdateFindings` per aggiornare i seguenti campi e oggetti:

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Configurazione dell'accesso a BatchUpdateFindings

È possibile configurare le policy AWS Identity and Access Management (IAM) per limitare l'accesso all'utilizzo per `BatchUpdateFindings` aggiornare i campi di ricerca e i valori dei campi.

In un'istruzione a cui limitare l'accesso`BatchUpdateFindings`, utilizza i seguenti valori:

- `Action` è `securityhub:BatchUpdateFindings`
- `Effect` è `Deny`
- Infatti`Condition`, puoi rifiutare una `BatchUpdateFindings` richiesta in base a quanto segue:
  - La scoperta include un campo specifico.
  - Il risultato include un valore di campo specifico.

Chiavi di condizione

Queste sono le chiavi condizionali per limitare l'accesso a`BatchUpdateFindings`.

Campo ASFF

La chiave di condizione per un campo ASFF è la seguente:

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Sostituisci *<fieldName>* con il campo ASFF. Quando configuri l'accesso a`BatchUpdateFindings`, includi uno o più campi ASFF specifici nella tua policy IAM anziché un campo a livello principale. Ad esempio, per limitare l'accesso al `Workflow.Status` campo, devi includere `securityhub:ASFFSyntaxPath/Workflow.Status` nella tua policy anziché il campo a livello principale. `Workflow`

Impedire tutti gli aggiornamenti a un campo

Per impedire a un utente di apportare aggiornamenti a un campo specifico, utilizza una condizione come questa:

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
               }
}
```

Ad esempio, la seguente dichiarazione indica che non `BatchUpdateFindings` può essere utilizzata per aggiornare il `Workflow.Status` campo dei risultati.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

Non consentire valori di campo specifici

Per impedire a un utente di impostare un campo su un valore specifico, usa una condizione come questa:

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
                }
}
```

Ad esempio, la seguente istruzione indica che non `BatchUpdateFindings` può essere utilizzata per `Workflow.Status` impostare su`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

Puoi anche fornire un elenco di valori non consentiti.

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
                }
}
```

Ad esempio, la seguente dichiarazione indica che non `BatchUpdateFindings` può essere utilizzata per `Workflow.Status` impostare uno dei due `RESOLVED` valori`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
```

```
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

Revisione dei dettagli e della cronologia dei risultati in Security Hub CSPM

In AWS Security Hub CSPM, un risultato è una registrazione osservabile di un controllo di sicurezza o di un rilevamento relativo alla sicurezza. Security Hub CSPM genera un risultato quando completa un controllo di sicurezza e quando inserisce un risultato da un prodotto integrato Servizio AWS o di terze parti. Ogni risultato include una cronologia delle modifiche e altri dettagli, come un indice di gravità e informazioni sulle risorse interessate.

Puoi rivedere la cronologia e altri dettagli dei singoli risultati sulla console CSPM di Security Hub o a livello di codice con l'API CSPM di Security Hub o il. AWS CLI

Per aiutarti a semplificare l'analisi, la console Security Hub CSPM visualizza un pannello di ricerca quando scegli un risultato specifico. Il pannello include diversi menu e schede per esaminare i dettagli specifici di un risultato.

Menu Azioni

Da questo menu è possibile rivedere il codice JSON completo di una ricerca o aggiungere note. A un risultato può essere allegata una sola nota alla volta. Questo menu fornisce anche opzioni per impostare lo stato del flusso di lavoro di un risultato o inviare un risultato a un'azione personalizzata in Amazon EventBridge.

Esplora il menu

Da questo menu, puoi esaminare una scoperta in Amazon Detective. Detective estrae entità, come indirizzi IP e AWS utenti, da una scoperta e visualizza la loro attività. È possibile utilizzare l'attività dell'entità come punto di partenza per indagare sulla causa e sull'impatto di una scoperta.

Scheda Panoramica

Questa scheda fornisce un riepilogo di un risultato. Ad esempio, è possibile determinare quando un risultato è stato creato e aggiornato l'ultima volta, in quale account esiste e l'origine del

risultato. Per quanto riguarda i risultati del controllo, questa scheda mostra anche il nome della AWS Config regola associata e un collegamento alle linee guida per la correzione nella documentazione CSPM di Security Hub.

Nell'istantanea delle risorse della scheda Panoramica, è possibile ottenere una breve panoramica delle risorse coinvolte in un risultato. Per alcune risorse, è inclusa l'opzione Open resource, che si collega direttamente a una risorsa interessata sulla console Servizio AWS pertinente. L'istantanea della cronologia mostra fino a due modifiche apportate al risultato nella data più recente per la quale viene tenuta traccia della cronologia. Ad esempio, se hai apportato una modifica ieri e un'altra oggi, l'istantanea mostra la modifica odierna. Per rivedere le voci precedenti, passa alla scheda Cronologia.

La riga Conformità si espande per mostrare ulteriori dettagli. Ad esempio, se un controllo include parametri, è possibile rivedere i valori dei parametri attualmente utilizzati da Security Hub CSPM per eseguire i controlli di sicurezza per il controllo.

Scheda Risorse

Questa scheda fornisce dettagli sulle risorse coinvolte in un risultato. Se hai effettuato l'accesso all'account che possiede una risorsa, puoi esaminarla nella Servizio AWS console pertinente. Se non sei il proprietario di una risorsa, questa scheda mostra l' Account AWS ID del proprietario.

La riga Dettagli mostra i dettagli specifici della risorsa in un risultato. Mostra la ResourceDetailssezione del risultato in formato JSON.

La riga Tag mostra le chiavi e i valori dei tag assegnati alle risorse coinvolte in un risultato. Le risorse supportate dal GetResources funzionamento dell'API AWS Resource Groups Tagging possono essere taggate. Security Hub CSPM richiama questa operazione utilizzando un ruolo collegato al servizio durante l'elaborazione di risultati nuovi o aggiornati e recupera i tag delle risorse se il campo AWS Security Finding Format (ASFF) `Resource.Id` è popolato con l'ARN di una risorsa. Security Hub CSPM ignora gli ID di risorsa non validi. Per ulteriori informazioni sull'inclusione dei tag di risorsa nei risultati, vedere. Tag

Scheda Cronologia

Questa scheda tiene traccia della cronologia di un ritrovamento. La cronologia delle ricerche è disponibile per i risultati attivi e archiviati. Fornisce una traccia immutabile delle modifiche apportate a un risultato nel tempo, tra cui la modifica del campo ASFF, quando è avvenuta la modifica e da quale utente. Ogni pagina della scheda mostra fino a 20 modifiche. Le modifiche più recenti vengono visualizzate per prime.

Per i risultati attivi, la cronologia dei risultati è disponibile per un massimo di 90 giorni. Per i risultati archiviati, la cronologia dei risultati è disponibile per un massimo di 30 giorni. La ricerca della cronologia include le modifiche apportate manualmente o automaticamente dalle regole di automazione CSPM di Security Hub. Non include le modifiche ai campi di timestamp di primo livello, come i campi e. `CreatedAt` `UpdatedAt`

Se hai effettuato l'accesso a un account amministratore CSPM di Security Hub, la cronologia delle ricerche riguarda l'account amministratore e tutti gli account dei membri.

Scheda Minacce

Questa scheda include i dati e ProcessDetailsgli oggetti dell'ASFF, incluso il tipo di minaccia e se una risorsa è l'obiettivo o l'attore. ActionMalware Questi dettagli si applicano in genere ai risultati che provengono da Amazon GuardDuty.

Scheda Vulnerabilità

Questa scheda mostra i dati dell'Vulnerabilityoggetto dell'ASFF, inclusa l'eventuale presenza di exploit o correzioni disponibili associati a un risultato. Questi dettagli si applicano in genere ai risultati che provengono da Amazon Inspector.

Le righe di ogni scheda includono un'opzione di copia o filtro. Ad esempio, se aprite il pannello relativo a un risultato con lo stato del flusso di lavoro impostato su Notificato, potete scegliere l'opzione di filtro accanto alla riga Stato del flusso di lavoro. Se scegli Mostra tutti i risultati con questo valore, Security Hub CSPM filtra la tabella dei risultati e visualizza solo i risultati con lo stesso stato del flusso di lavoro.

Revisione dei dettagli e della cronologia dei risultati

Scegli il tuo metodo preferito e segui i passaggi per esaminare i dettagli della ricerca in Security Hub CSPM.

Se abiliti l'aggregazione tra regioni e accedi alla regione di aggregazione, la ricerca dei dati include i dati della regione di aggregazione e delle regioni collegate. In altre regioni, la ricerca di dati è specifica solo per quella regione. Per ulteriori informazioni sull'aggregazione tra regioni, vedere. the section called “Aggregazione dei dati tra le regioni”

Security Hub CSPM console

Analisi dei dettagli e della cronologia dei risultati

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Per visualizzare un elenco dei risultati, effettuate una delle seguenti operazioni:
   - Nel riquadro di navigazione, seleziona Esiti. Aggiungete i filtri di ricerca necessari per restringere l'elenco dei risultati.
   - Nel riquadro di navigazione, seleziona Informazioni dettagliate. Scegli un approfondimento. Quindi, nell'elenco dei risultati, scegli un risultato approfondito.
   - Nel riquadro di navigazione, scegli Integrazioni. Scegli Vedi risultati per un'integrazione.
   - Nel riquadro di navigazione, scegli Controlli.
3. Scegli un risultato. Il pannello di ricerca mostra i dettagli del risultato.
4. Nel pannello di ricerca, effettuate una delle seguenti operazioni:
   - Per esaminare i dettagli specifici del risultato, scegliete una scheda.
   - Per intervenire sulla scoperta, scegli un'opzione dal menu Azioni.
   - Per indagare sulla scoperta in Amazon Detective, scegli un'opzione Investigate.

> **Note**
>
> Se esegui l'integrazione con AWS Organizations e hai effettuato l'accesso a un account membro, il pannello di ricerca include il nome dell'account. Per gli account membro invitati manualmente, anziché tramite Organizations, il pannello di ricerca include solo l'ID dell'account.

Security Hub CSPM API

Utilizza il GetFindingsfunzionamento dell'API CSPM Security Hub o, se stai utilizzando AWS CLI, esegui il comando. get-findings Puoi fornire uno o più valori per il `Filters` parametro per restringere i risultati da recuperare.

Se il volume dei risultati è troppo grande, è possibile utilizzare il `MaxResults` parametro per limitare i risultati a un numero specifico e il `NextToken` parametro per impaginare i risultati. Utilizzate il `SortCriteria` parametro per ordinare i risultati in base a un campo specifico.

Ad esempio, il AWS CLI comando seguente recupera i risultati che corrispondono ai criteri di filtro specificati e ordina i risultati in ordine decrescente in base al campo. `LastObservedAt` Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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
```

Per esaminare la cronologia dei risultati, utilizzare l'operazione. GetFindingHistory Se stai usando il AWS CLI, esegui il get-finding-historycomando. Identifica il risultato di cui vuoi ottenere la cronologia con i `Id` campi `ProductArn` and. Per informazioni su questi campi, consulta AwsSecurityFindingIdentifier. Ogni richiesta può recuperare la cronologia di un solo risultato.

Ad esempio, il AWS CLI comando seguente recupera la cronologia del risultato specificato. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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

Utilizza il cmdlet `Get-SHUBFinding`. Facoltativamente, compila il `Filter` parametro per restringere i risultati da recuperare.

Ad esempio, il cmdlet seguente recupera i risultati che corrispondono ai filtri specificati.

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> Se si filtrano i risultati per `CompanyName` o`ProductName`, Security Hub CSPM utilizza i valori che fanno parte dell'oggetto `ProductFields` ASFF. Security Hub CSPM non utilizza il livello e i campi principali`CompanyName`. `ProductName`

Filtraggio dei risultati in Security Hub CSPM

AWS Security Hub CSPM genera i propri risultati dai controlli di sicurezza e riceve i risultati dai prodotti integrati. È possibile visualizzare un elenco di risultati nelle pagine Findings, Integrations e Insights della console Security Hub CSPM. È possibile aggiungere filtri per restringere un elenco di risultati in modo che l'elenco sia pertinente alla propria organizzazione o al proprio caso d'uso.

Per informazioni sul filtraggio dei risultati per uno specifico controllo di sicurezza, consultathe section called "Filtraggio e ordinamento dei risultati del controllo". Le informazioni contenute in questa pagina si riferiscono alle pagine Findings, Insights e Integrations.

Filtri predefiniti per gli elenchi di ricerca

Per impostazione predefinita, gli elenchi di ricerca sulla console CSPM di Security Hub vengono filtrati in base ai `Workflow.Status` campi `RecordState` e del AWS Security Finding Format (ASFF). Questo si aggiunge ai filtri per informazioni o integrazioni specifiche.

Lo stato del record indica se un risultato è attivo o archiviato. Per impostazione predefinita, un elenco di risultati mostra solo i risultati attivi. Un fornitore di servizi di ricerca può archiviare un risultato se non è più attivo o importante. Security Hub CSPM archivia inoltre automaticamente i risultati del controllo se la risorsa associata viene eliminata.

Lo stato del flusso di lavoro indica lo stato di un'indagine su un risultato. Per impostazione predefinita, un elenco di risultati mostra solo risultati con uno stato del flusso di lavoro `NEW` o `NOTIFIED`. È possibile aggiornare lo stato del flusso di lavoro di un risultato.

Istruzioni per aggiungere filtri

È possibile filtrare un elenco di risultati in base a un massimo di dieci attributi. Per ogni attributo, puoi fornire fino a 20 valori di filtro.

Quando filtra l'elenco dei risultati, Security Hub CSPM applica la `AND` logica al set di filtri. Una ricerca corrisponde solo se corrisponde a tutti i filtri forniti. Ad esempio, se si aggiunge GuardDuty come filtro per il nome del prodotto e `AwsS3Bucket` come filtro per il tipo di risorsa, Security Hub CSPM visualizza i risultati che soddisfano entrambi questi criteri.

Security Hub CSPM applica `OR` la logica ai filtri che utilizzano lo stesso attributo ma valori diversi. Ad esempio, se aggiungi entrambi GuardDuty e Amazon Inspector come valori di filtro per Product name, Security Hub CSPM visualizza i risultati generati da Amazon Inspector o da Amazon GuardDuty Inspector.

Per aggiungere filtri a un elenco di risultati (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Per visualizzare un elenco dei risultati, esegui una delle seguenti azioni dal pannello di navigazione:
   - Scegli Findings.
   - Scegli Approfondimenti. Scegli un approfondimento. Quindi, nell'elenco dei risultati, scegli un risultato approfondito.
   - Scegli Integrations (Integrazioni). Scegli Vedi risultati per un'integrazione.
3. Nella casella Aggiungi filtri, seleziona uno o più campi in base ai quali filtrare.

   Quando si filtra in base al nome dell'azienda o al nome del prodotto, la console utilizza il livello superiore `CompanyName` e `ProductName` i campi del AWS Security Finding Format (ASFF). L'API utilizza i valori in cui sono annidati. `ProductFields`
4. Scegliere il tipo di corrispondenza del filtro.

   Per un filtro a stringa, puoi scegliere tra le seguenti opzioni:
   - is — Trova un valore che corrisponda esattamente al valore del filtro.
   - inizia con: trova un valore che inizi con il valore del filtro.
   - non è: trova un valore che non corrisponde al valore del filtro.

- non inizia con: trova un valore che non inizia con il valore del filtro.

Per il campo Tag delle risorse, puoi filtrare in base a chiavi o valori specifici.

Per un filtro numerico, puoi scegliere se fornire un numero singolo (Semplice) o un intervallo di numeri (Range).

Per un filtro di data o ora, puoi scegliere se fornire un intervallo di tempo compreso tra la data e l'ora correnti (finestra scorrevole) o un intervallo di date specifico (intervallo fisso).

L'aggiunta di più filtri comporta le seguenti interazioni:

- is e inizia con i filtri sono uniti da OR. Un valore corrisponde se contiene uno qualsiasi dei valori del filtro. Ad esempio, se si specifica che l'etichetta di gravità è CRITICA e l'etichetta di gravità è ALTA, i risultati includono sia i risultati critici che quelli ad alta gravità.
- non è e non inizia con i filtri vengono uniti da AND. Un valore corrisponde solo se non contiene nessuno di questi valori di filtro. Ad esempio, se si specifica che l'etichetta di gravità non è LOW e l'etichetta di severità non è MEDIUM, i risultati non includono i risultati di gravità bassa o media.

Se hai un filtro is su un campo, non puoi avere un filtro is no o un non inizia con un filtro sullo stesso campo.

5. Specificare il valore del filtro. Per i filtri a stringa, il valore del filtro fa distinzione tra maiuscole e minuscole.
6. Scegli Applica.

Per un filtro esistente, è possibile modificare il tipo o il valore della corrispondenza del filtro. In un elenco di risultati filtrato, scegli il filtro. Nella casella Modifica filtro, scegli il nuovo tipo o valore di corrispondenza, quindi scegli Applica.

Per rimuovere un filtro, scegli l'icona x. L'elenco viene aggiornato automaticamente in base alla modifica.

Raggruppamento dei risultati in Security Hub CSPM

È possibile raggruppare i risultati in AWS Security Hub CSPM in base ai valori di un attributo selezionato.

Quando si raggruppano i risultati, l'elenco dei risultati viene sostituito con un elenco di valori per l'attributo selezionato nei risultati corrispondenti. Per ogni valore, l'elenco mostra il numero di risultati corrispondenti.

Ad esempio, se si raggruppano i risultati per Account AWS ID, viene visualizzato un elenco di identificatori di account, con il numero di risultati corrispondenti per ogni account.

Security Hub CSPM può visualizzare fino a 100 valori per un attributo selezionato. Se sono presenti più di 100 valori, vengono visualizzati solo i primi 100.

Quando si sceglie un valore di attributo, Security Hub CSPM visualizza l'elenco dei risultati corrispondenti per quel valore.

Per raggruppare i risultati in un elenco di risultati (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Per visualizzare un elenco dei risultati, esegui una delle seguenti azioni dal pannello di navigazione:
   - Scegli Findings.
   - Scegli Approfondimenti. Scegli un approfondimento. Quindi, nell'elenco dei risultati, scegli un risultato approfondito.
   - Scegli Integrations (Integrazioni). Scegli Vedi risultati per un'integrazione.
3. Nel menu a discesa Raggruppa per, scegli l'attributo da utilizzare per il raggruppamento.

   Per rimuovere un attributo di raggruppamento, scegli l'icona x. Quando rimuovete l'attributo di raggruppamento, l'elenco passa dall'elenco dei valori degli attributi a un elenco di risultati.

Impostazione dello stato del flusso di lavoro dei risultati in Security Hub CSPM

Lo stato del flusso di lavoro tiene traccia dello stato di avanzamento dell'indagine su un risultato. Lo stato del flusso di lavoro è specifico per una singola scoperta e non influisce sulla generazione di nuovi risultati. Ad esempio, se si modifica lo stato del flusso di lavoro di un risultato in `SUPPRESSED` o`RESOLVED`, la modifica non impedisce a Security Hub CSPM di generare un nuovo risultato per lo stesso problema.

Lo stato del flusso di lavoro di un risultato può corrispondere a uno dei seguenti valori.

NUOVO

Lo stato iniziale di un risultato prima di esaminarlo.

I risultati che vengono acquisiti da sistemi integrati Servizi AWS, ad esempio AWS Config, hanno `NEW` come stato iniziale.

Security Hub CSPM reimposta inoltre lo stato del flusso di lavoro da uno `NOTIFIED` o `RESOLVED` a `NEW` nei seguenti casi:

- `RecordState`cambia da a. `ARCHIVED` `ACTIVE`
- `Compliance.Status`modifiche da `PASSED` a `FAILEDWARNING`, o`NOT_AVAILABLE`.

Queste modifiche implicano la necessità di ulteriori indagini.

NOTIFICATO

Indica che il problema di sicurezza è stato notificato al proprietario della risorsa. Puoi utilizzare questo stato quando non sei il proprietario della risorsa ed è necessario l'intervento del proprietario della risorsa per risolvere un problema di sicurezza.

Se si verifica una delle seguenti condizioni, lo stato del flusso di lavoro viene modificato automaticamente da `NOTIFIED` a`NEW`:

- `RecordState`cambia da `ARCHIVED` a`ACTIVE`.
- `Compliance.Status`modifiche da `PASSED` a `FAILEDWARNING`, o`NOT_AVAILABLE`.

SOPPRESSO

Indica che hai esaminato la scoperta e che non ritieni necessaria alcuna azione.

Lo stato del flusso di lavoro di un `SUPPRESSED` risultato non cambia se `RecordState` cambia da `ARCHIVED` a`ACTIVE`.

RISOLTO

Il risultato è stato esaminato e corretto ed è ora considerato risolto.

Il risultato rimane valido `RESOLVED` a meno che non si verifichi una delle seguenti condizioni:

- `RecordState`cambia da `ARCHIVED` a`ACTIVE`.
- `Compliance.Status`modifiche da `PASSED` a `FAILEDWARNING`, o`NOT_AVAILABLE`.

In questi casi, lo stato del flusso di lavoro viene reimpostato automaticamente su`NEW`.

Per i risultati dei controlli, in caso `Compliance.Status` affermativo`PASSED`, Security Hub CSPM imposta automaticamente lo stato del flusso di lavoro su. `RESOLVED`

Impostazione dello stato dei risultati del flusso di lavoro

Per modificare lo stato del flusso di lavoro di uno o più risultati, puoi utilizzare la console CSPM di Security Hub o l'API CSPM di Security Hub. Se modifichi lo stato del flusso di lavoro di un risultato, tieni presente che Security Hub CSPM potrebbe impiegare diversi minuti per elaborare la richiesta e aggiornare il risultato.

> **Tip**
>
> È inoltre possibile modificare automaticamente lo stato del flusso di lavoro dei risultati utilizzando le regole di automazione. Con le regole di automazione, configuri Security Hub CSPM per aggiornare automaticamente lo stato del flusso di lavoro dei risultati in base ai criteri specificati. Per ulteriori informazioni, consulta Comprensione delle regole di automazione in Security Hub CSPM.

Per modificare lo stato del flusso di lavoro di uno o più risultati, scegli il metodo preferito e segui i passaggi.

Security Hub CSPM console

Per modificare lo stato dei risultati del flusso di lavoro

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, effettuate una delle seguenti operazioni per visualizzare una tabella dei risultati:
   - Scegliete Findings.
   - Scegli Approfondimenti. Quindi scegli un approfondimento. Nei risultati dell'analisi, scegli un risultato.
   - Scegli Integrations (Integrazioni). Quindi, nella sezione relativa all'integrazione, scegli Vedi risultati.

- Scegli gli standard di sicurezza. Quindi, nella sezione relativa allo standard, scegli Visualizza risultati. Nella tabella dei controlli, scegli un controllo per visualizzare i risultati relativi al controllo.

3. Nella tabella dei risultati, seleziona la casella di controllo per ogni risultato di cui desideri modificare lo stato del flusso di lavoro.
4. Nella parte superiore della pagina, scegli Stato del flusso di lavoro, quindi scegli il nuovo stato del flusso di lavoro per i risultati selezionati.
5. Nella finestra di dialogo Imposta lo stato del flusso di lavoro, inserisci facoltativamente una nota che descriva in dettaglio il motivo della modifica dello stato del flusso di lavoro. Quindi scegli Imposta stato.

Security Hub CSPM API

Usa l'BatchUpdateFindingsoperazione. Fornisci sia l'ID del risultato che l'ARN del prodotto che ha generato il risultato. È possibile ottenere questi dettagli utilizzando l'GetFindingsoperazione.

AWS CLI

Esegui il comando batch-update-findings. Fornisci sia l'ID del risultato che l'ARN del prodotto che ha generato il risultato. È possibile ottenere questi dettagli eseguendo il comando get-finding.

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Esempio

```
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"
```

Invio dei risultati a un'azione CSPM personalizzata di Security Hub

Puoi creare azioni personalizzate AWS Security Hub CSPM per automatizzare Security Hub CSPM con Amazon. EventBridge Per le operazioni personalizzate, il tipo di evento è Security Hub Findings - Custom Action. Dopo aver impostato un'operazione personalizzata, puoi inviare risultati. Per ulteriori

informazioni e fasi dettagliate sulla creazione di operazioni personalizzate, consulta the section called "Risposta e riparazione automatiche".

Per inviare i risultati a un'azione personalizzata (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Per visualizzare un elenco dei risultati, effettuate una delle seguenti operazioni:
   - Nel riquadro di navigazione CSPM di Security Hub, scegli Findings.
   - Nel riquadro di navigazione CSPM di Security Hub, scegli Insights. Scegli un approfondimento. Quindi, nell'elenco dei risultati, scegli un risultato approfondito.
   - Nel pannello di navigazione CSPM di Security Hub, scegli Integrazioni. Scegli Vedi i risultati per un'integrazione.
   - Nel pannello di navigazione CSPM di Security Hub, scegli Standard di sicurezza. Scegli Visualizza risultati per visualizzare un elenco di controlli. Quindi scegli il nome del controllo.
3. Nell'elenco dei risultati, seleziona la casella di controllo relativa a ciascun risultato da inviare all'azione personalizzata.

   È possibile inviare fino a 20 risultati alla volta.
4. Per Azioni, scegli l'azione personalizzata.

AWS Formato ASFF (Security Finding Format)

AWS Security Hub CSPM utilizza e aggrega i risultati di prodotti integrati Servizi AWS e di terze parti. Security Hub CSPM elabora questi risultati utilizzando un formato di risultati standard chiamato AWS Security Finding Format (ASFF), che elimina la necessità di lunghi sforzi di conversione dei dati.

Questa pagina fornisce una descrizione completa del codice JSON relativo a un risultato del AWS Security Finding Format (ASFF). Il formato deriva da JSON Schema. Scegliete il nome di un oggetto collegato per esaminare un esempio di scoperta per quell'oggetto. Il confronto dei risultati del Security Hub CSPM con le risorse e gli esempi mostrati qui può aiutarti a interpretare i risultati.

Per le descrizioni dei singoli attributi ASFF, vedere e. the section called "Attributi ASFF di primo livello obbligatori" the section called "Attributi ASFF di primo livello opzionali"

```
"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"
    }
```

```
]
```

Impatto del consolidamento sui campi e sui valori ASFF

AWS Security Hub CSPM offre due tipi di consolidamento per i controlli:

- Visualizzazione consolidata dei controlli: con questo tipo di consolidamento, ogni controllo ha un unico identificatore per tutti gli standard. Inoltre, nella console Security Hub CSPM, la pagina Controlli mostra tutti i controlli di tutti gli standard.
- Risultati di controllo consolidati: con questo tipo di consolidamento, Security Hub CSPM produce un'unica ricerca per un controllo, anche se il controllo si applica a più standard abilitati. Questo può ridurre il rumore di ricerca.

Non è possibile abilitare o disabilitare la visualizzazione dei controlli consolidati. I risultati del controllo consolidato sono abilitati per impostazione predefinita se abiliti Security Hub CSPM a partire dal 23 febbraio 2023. Altrimenti, è disabilitato per impostazione predefinita. Tuttavia, per le organizzazioni, i risultati del controllo consolidato sono abilitati per gli account dei membri CSPM di Security Hub solo se sono abilitati per l'account amministratore. Per ulteriori informazioni sui risultati del controllo consolidato, consulta. Generazione e aggiornamento dei risultati di controllo

Entrambi i tipi di consolidamento influiscono sui campi e sui valori dei risultati di controllo in. AWS Formato ASFF (Security Finding Format)

Argomenti

- Visualizzazione consolidata dei controlli: modifiche ASFF
- Risultati di controllo consolidati: modifiche ASFF
- ID del generatore prima e dopo l'attivazione dei risultati di controllo consolidati
- In che modo il consolidamento influisce sugli ID e sui titoli di controllo
- Aggiornamento dei flussi di lavoro per il consolidamento

Visualizzazione consolidata dei controlli: modifiche ASFF

La funzionalità di visualizzazione dei controlli consolidati ha introdotto le seguenti modifiche ai campi e ai valori relativi ai risultati dei controlli nell'ASFF. Se i flussi di lavoro non si basano sui valori di questi campi ASFF, non è richiesta alcuna azione. Se disponi di flussi di lavoro che si basano su valori specifici per questi campi, aggiorna i flussi di lavoro per utilizzare i valori correnti.

Campo ASFF	Valore di esempio prima della visualizzazione dei controlli consolidati	Valore di esempio dopo la visualizzazione dei controlli consolidati e descrizione della modifica
Compliance.SecurityControlId	Non applicabile (nuovo campo)	EC2.2 Introduce un unico ID di controllo per tutti gli standard. `ProductFields.RuleId` fornisce ancora l'ID di controllo basato su standard per i controlli CIS v1.2.0. `ProductFields.ControlId` fornisce ancora l'ID di controllo basato su standard per i controlli di altri standard.
Compliance.AssociatedStandards	Non applicabile (nuovo campo)	[{» StandardsId «:" standards /aws -foundational-security-best- /1.0.0 «}] practices/v Mostra in quali standard è abilitato un controllo.
ProductFields.ArchivalReasons:0/Description	Non applicabile (nuovo campo)	«Il risultato è in uno stato ARCHIVIATO perché i risultati del controllo consolidato sono stati attivati o disattivati. Ciò fa sì che i risultati dello stato precedente vengano archiviati quando vengono generati nuovi risultati». Descrive perché Security Hub CSPM ha archiviato i risultati esistenti.

Campo ASFF	Valore di esempio prima della visualizzazione dei controlli consolidati	Valore di esempio dopo la visualizzazione dei controlli consolidati e descrizione della modifica
ProductFields.ArchivalReasons:0/ReasonCode	Non applicabile (nuovo campo)	«CONSOLIDATED_CONTROL_FINDINGS_UPDATE» Fornisce il motivo per cui Security Hub CSPM ha archiviato i risultati esistenti.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Questo campo non fa più riferimento a uno standard.
Remediation.Recommendation.Text	«Per istruzioni su come risolvere questo problema, consulta la documentazione PCI AWS DSS di Security Hub CSPM.»	«Per istruzioni su come correggere questo problema, consulta la documentazione sui controlli CSPM AWS di Security Hub.» Questo campo non fa più riferimento a uno 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 Questo campo non fa più riferimento a uno standard.

Risultati di controllo consolidati: modifiche ASFF

Se abiliti i risultati di controllo consolidati, potrebbero interessarti le seguenti modifiche ai campi e ai valori relativi ai risultati di controllo nell'ASFF. Queste modifiche si aggiungono a quelle introdotte dalla funzionalità di visualizzazione dei controlli consolidati. Se i flussi di lavoro non si basano sui valori di questi campi ASFF, non è richiesta alcuna azione. Se disponi di flussi di lavoro che si basano su valori specifici per questi campi, aggiorna i flussi di lavoro per utilizzare i valori correnti.

> **Tip**
>
> Se utilizzi la soluzione Automated Security Response on AWS v2.0.0, tieni presente che supporta i risultati del controllo consolidato. Ciò significa che è possibile mantenere i flussi di lavoro attuali se si abilitano i risultati di controllo consolidati.

Campo ASFF	Valore di esempio prima di abilitare i risultati di controllo consolidati	Valore di esempio dopo aver abilitato i risultati del controllo consolidato e una descrizione della modifica
GeneratorId	aws-foundational-security-best- /1.0. practices/v 0/Config.1	sicurezza- 1. control/Config Questo campo non fa più riferimento a uno standard.
Titolo	PCI.Config.1 AWS Config dovrebbe essere abilitato	AWS Config dovrebbe essere abilitato Questo campo non fa più riferimento a informazioni specifiche dello standard.
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: sicurezza-. control/iam 9/finding/ab6d6a26-a156-48f0-9403-115983e5a956

Campo ASFF	Valore di esempio prima di abilitare i risultati di controllo consolidati	Valore di esempio dopo aver abilitato i risultati del controllo consolidato e una descrizione della modifica
		Questo campo non fa più riferimento a uno standard.
ProductFields.ControlId	PCI.EC2.2	Rimosso. Vedi `Compliance.SecurityControlId` invece. Questo campo viene rimosso a favore di un unico ID di controllo indipendente dagli standard.
ProductFields.RuleId	1.3	Rimosso. Vedi `Compliance.SecurityControlId` invece. Questo campo viene rimosso a favore di un unico ID di controllo indipendente dagli standard.
Description	Questo controllo PCI DSS verifica se AWS Config è abilitato nell'account e nella regione correnti.	Questo AWS controllo verifica se AWS Config è abilitato nell'account e nella regione correnti. Questo campo non fa più riferimento a uno standard.

Campo ASFF	Valore di esempio prima di abilitare i risultati di controllo consolidati	Valore di esempio dopo aver abilitato i risultati del controllo consolidato e una descrizione della modifica

Gravità	«Severità»: {
	«Prodotto»: 90,
	«Etichetta»: «CRITICAL»,
	«Normalizzato»: 90,
	«Originale»: «CRITICO»
	}
		«Severità»: {
		«Etichetta»: «CRITICAL»,
		«Normalizzato»: 90,
		«Originale»: «CRITICO»
		}
		Security Hub CSPM non utilizza più il campo Prodotto per descrivere la gravità di un risultato.

Tipi	["Software, configurazione Checks/Industry e regolamen tazione Standards/PCI-DSS «]	["Software e configurazione Checks/Industry e standard normativi"] Questo campo non fa più riferimento a uno standard.
Compliance.Related Requirements	["PCI DSS 10.5.2", «PCI DSS 11,5", « AWS Fondazioni CIS 2.5"]	["PCI DSS versione 3.2. 1/101,5,2 ", «PCI DSS versione 3.2. 1/111,5", «Benchmark CIS AWS Foundatio ns v1.2. 0/2[5"] Questo campo mostra i requisiti correlati in tutti gli standard abilitati.

Campo ASFF	Valore di esempio prima di abilitare i risultati di controllo consolidati	Valore di esempio dopo aver abilitato i risultati del controllo consolidato e una descrizione della modifica
CreatedAt	2022-05-05 T08:18:13.138Z	2022-09-25 T08:18:13.138Z Il formato rimane lo stesso, ma il valore viene ripristinato quando si abilitano i risultati del controllo consolidato.
FirstObservedAt	2022-05-07 T08:18:13.138Z	2022-09-28 T08:18:13.138Z Il formato rimane lo stesso, ma il valore viene ripristinato quando si abilitano i risultati del controllo consolidato.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	Rimosso. Vedi `Remediation.Recommendation.Url` invece.
ProductFields.StandardsArn	arn:aws:securityhub::: -foundational-security-best- /1.0.0 standards/aws practices/v	Rimosso. Vedi `Compliance.AssociatedStandards` invece.
ProductFields.StandardsControlArn	arn:aws:securityhub:us-east-1:123456789012: -foundational-security-best- /1.0. control/aws practices/v 0/Config.1	Rimosso. Security Hub CSPM genera un risultato per un controllo di sicurezza tra gli standard.
ProductFields.StandardsGuideArn	arn:aws:securityhub::: -aws-foundation- /1.2.0 ruleset/cis benchmark/v	Rimosso. Vedi `Compliance.AssociatedStandards` invece.

Campo ASFF	Valore di esempio prima di abilitare i risultati di controllo consolidati	Valore di esempio dopo aver abilitato i risultati del controllo consolidato e una descrizione della modifica
ProductFields.StandardsGuideSubscriptionArn	arn:aws:securityhub:us-east-2:123456789012: -aws-foundations-/1.2.0 subscription/cis benchmark/v	Rimosso. Security Hub CSPM genera un risultato per un controllo di sicurezza tra gli standard.
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012: -foundational-security-best- /1.0.0 subscription/ aws practices/v	Rimosso. Security Hub CSPM genera un risultato per un controllo di sicurezza tra gli standard.
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: sicurezza-. product/aws securityhub/arn control/Config 1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 Questo campo non fa più riferimento a uno standard.

Valori per i campi ASFF forniti dal cliente dopo l'attivazione dei risultati del controllo consolidato

Se abiliti i risultati del controllo consolidato, Security Hub CSPM genera un risultato tra gli standard e archivia i risultati originali (risultati separati per ogni standard).

Gli aggiornamenti apportati ai risultati originali utilizzando la console CSPM di Security Hub o l'BatchUpdateFindingsoperazione non verranno conservati nei nuovi risultati. Se necessario, puoi recuperare questi dati facendo riferimento ai risultati archiviati. Per esaminare i risultati archiviati, è possibile utilizzare la pagina Risultati sulla console CSPM di Security Hub e impostare il filtro Record state su ARCHIVED. In alternativa, è possibile utilizzare il GetFindingsfunzionamento dell'API CSPM Security Hub.

Customer-provided Campo ASFF	Descrizione della modifica dopo l'attivazione dei risultati di controllo consolidati
Confidence	Ripristina lo stato vuoto.
Criticità	Si ripristina allo stato vuoto.
Nota	Si ripristina allo stato vuoto.
RelatedFindings	Si ripristina allo stato vuoto.
Gravità	Gravità predefinita del risultato (corrisponde alla gravità del controllo).
Tipi	Ripristina il valore indipendente dallo standard.
UserDefinedFields	Ripristina lo stato vuoto.
VerificationState	Si ripristina allo stato vuoto.
Flusso di lavoro	Il valore predefinito dei nuovi risultati non riusciti è. `NEW` I nuovi risultati passati hanno un valore predefinito di`RESOLVED`.

ID del generatore prima e dopo l'attivazione dei risultati di controllo consolidati

La tabella seguente elenca le modifiche ai valori degli ID del generatore per i controlli quando abiliti i risultati del controllo consolidato. Queste modifiche si applicano ai controlli supportati da Security Hub CSPM a partire dal 15 febbraio 2023.

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/1.1	sicurezza- 1. control/CloudWatch
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/1.10	sicurezza- 1.6 control/IAM

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/1.11	sicurezza- .17 control/IAM
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/1.12	sicurezza- 4. control/IAM
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/1.13	sicurezza- 9. control/IAM
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/1.14	sicurezza- 6. control/IAM
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/1.16	sicurezza- 2. control/IAM
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/1.2	sicurezza- 5. control/IAM
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/1,20	sicurezza- .18 control/IAM
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/1,22	sicurezza- 1. control/IAM
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/1.3	sicurezza- 8. control/IAM
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/1.4	sicurezza- 3. control/IAM
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/1.5	sicurezza- .11 control/IAM
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/1.6	sicurezza- .12 control/IAM

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/1.7	sicurezza- 1.3 control/IAM
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/1.8	sicurezza- 1.4 control/IAM
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/1,9	sicurezza- 1.5 control/IAM
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/2.1	sicurezza- 1. control/CloudTrail
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/2.2	sicurezza- 4. control/CloudTrail
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/2.3	sicurezza- 6. control/CloudTrail
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/2.4	sicurezza- 5. control/CloudTrail
arn:aws:securityhub::: -aws-foundations-/1.2. ruleset/cis benchmark/v 0/rule/2.5	sicurezza- 1. control/Config
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/2.6	sicurezza- 7. control/CloudTrail
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/2.7	sicurezza- 2. control/CloudTrail
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/2.8	sicurezza- 4. control/KMS
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/2,9	sicurezza- 6. control/EC2

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.1	sicurezza- 2. control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.2	sicurezza- 3. control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.3	sicurezza- 1. control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.4	sicurezza- 4. control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3,5	sicurezza- 5. control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.6	sicurezza- 6. control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.7	sicurezza- 7. control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.8	sicurezza- 8. control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.9	sicurezza- .9 control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.10	sicurezza- .10 control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.11	sicurezza- .11 control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.12	sicurezza- .12 control/CloudWatch

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.13	sicurezza- .13 control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/3.14	sicurezza- .14 control/CloudWatch
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/4.1	sicurezza- 1.3 control/EC2
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/4.2	sicurezza- 1.4 control/EC2
arn:aws:securityhub::: -aws-foundation- /1.2. ruleset/cis benchmark/v 0/rule/4.3	sicurezza- 2. control/EC2
cis-aws-foundation- /1.4. benchmark/v 0/1.10	sicurezza- 5. control/IAM
cis-aws-foundation- /1.4. benchmark/v 0/1.14	sicurezza- 3. control/IAM
cis-aws-foundation- /1.4. benchmark/v 0/1.16	sicurezza- 1. control/IAM
cis-aws-foundation- /1.4. benchmark/v 0/1.17	sicurezza- .18 control/IAM
cis-aws-foundation- /1.4. benchmark/v 0/1.4.	sicurezza- 4. control/IAM
cis-aws-foundation- /1.4. benchmark/v 0/15.	sicurezza- 9. control/IAM
cis-aws-foundation- /1.4. benchmark/v 0/16.	sicurezza- 6. control/IAM
cis-aws-foundation- /1.4. benchmark/v 0/17.	sicurezza- 1. control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/18.	sicurezza- .15 control/IAM
cis-aws-foundation- /1.4. benchmark/v 0/19.	sicurezza- .16 control/IAM
cis-aws-foundation- /1.4. benchmark/v 0/21.1.2	sicurezza- 5. control/S3
cis-aws-foundation- /1.4. benchmark/v 0/21.5.1	sicurezza- 1. control/S3

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
cis-aws-foundation- /1.4. benchmark/v 0/21.5.2	sicurezza- 8. control/S3
cis-aws-foundation- /1.4. benchmark/v 0/22.2.1	sicurezza- 7. control/EC2
cis-aws-foundation- /1.4. benchmark/v 0/23.3.1	sicurezza- 3. control/RDS
cis-aws-foundation- /1.4. benchmark/v 0/3.1	sicurezza- 1. control/CloudTrail
cis-aws-foundation- /1.4. benchmark/v 0/32.	sicurezza- 4. control/CloudTrail
cis-aws-foundation- /1.4. benchmark/v 0/3.4.	sicurezza- 5. control/CloudTrail
cis-aws-foundation- /1.4. benchmark/v 0/35.	sicurezza- 1. control/Config
cis-aws-foundation- /1.4. benchmark/v 0/36.	sicurezza- 9. control/S3
cis-aws-foundation- /1.4. benchmark/v 0/37.	sicurezza- 2. control/CloudTrail
cis-aws-foundation- /1.4. benchmark/v 0/38.	sicurezza- 4. control/KMS
cis-aws-foundation- /1.4. benchmark/v 0/39.	sicurezza- 6. control/EC2
cis-aws-foundation- /1.4. benchmark/v 0/43.	sicurezza- 1. control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/4.4.	sicurezza- 4. control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/45.	sicurezza- 5. control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/46.	sicurezza- 6. control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/47.	sicurezza- 7. control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/48.	sicurezza- 8. control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/49.	sicurezza- 9. control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/4.10	sicurezza- .10 control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/4.11	sicurezza- .11 control/CloudWatch

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
cis-aws-foundation- /1.4. benchmark/v 0/4.12	sicurezza- .12 control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/4.13	sicurezza- .13 control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/4.14	sicurezza- .14 control/CloudWatch
cis-aws-foundation- /1.4. benchmark/v 0/5.1	sicurezza- .21 control/EC2
cis-aws-foundation- /1.4. benchmark/v 0/53.	sicurezza- 2. control/EC2
aws-foundational-security-best-/1.0. practices/v 0/Account.1	sicurezza- 1. control/Account
aws-foundational-security-best-/1.0. practices/v 0/ACM.1	sicurezza- 1. control/ACM
aws-foundational-security-best-/1.0. practices/v 0/APIGateway.1	sicurezza- 1. control/APIGateway
aws-foundational-security-best-/1.0. practices/v 0/APIGateway2.	sicurezza- 2. control/APIGateway
aws-foundational-security-best-/1.0. practices/v 0/APIGateway3.	sicurezza- 3. control/APIGateway
aws-foundational-security-best-/1.0. practices/v 0/APIGateway4.	sicurezza- 4. control/APIGateway
aws-foundational-security-best-/1.0. practices/v 0/APIGateway5.	sicurezza- 5. control/APIGateway
aws-foundational-security-best-/1.0. practices/v 0/APIGateway8.	sicurezza- 8. control/APIGateway
aws-foundational-security-best-/1.0. practices/v 0/APIGateway9.	sicurezza- 9. control/APIGateway

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/AutoScaling.1	sicurezza- 1. control/AutoScaling
aws-foundational-security-best-/1.0. practices/v 0/AutoScaling2.	sicurezza- 2. control/AutoScaling
aws-foundational-security-best-/1.0. practices/v 0/AutoScaling3.	sicurezza- 3. control/AutoScaling
aws-foundational-security-best-/1.0. practices/v 0/Autoscaling5.	sicurezza- 5. control/Autoscaling
aws-foundational-security-best-/1.0. practices/v 0/AutoScaling6.	sicurezza- 6. control/AutoScaling
aws-foundational-security-best-/1.0. practices/v 0/AutoScaling9.	sicurezza- 9. control/AutoScaling
aws-foundational-security-best-/1.0. practices/v 0/CloudFront.1	sicurezza- 1. control/CloudFront
aws-foundational-security-best-/1.0. practices/v 0/CloudFront3.	sicurezza- 3. control/CloudFront
aws-foundational-security-best-/1.0. practices/v 0/CloudFront4.	sicurezza- 4. control/CloudFront
aws-foundational-security-best-/1.0. practices/v 0/CloudFront5.	sicurezza- 5. control/CloudFront
aws-foundational-security-best-/1.0. practices/v 0/CloudFront6.	sicurezza- 6. control/CloudFront
aws-foundational-security-best-/1.0. practices/v 0/CloudFront7.	sicurezza- 7. control/CloudFront

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/CloudFront8.	sicurezza- 8. control/CloudFront
aws-foundational-security-best-/1.0. practices/v 0/CloudFront9.	sicurezza- 9. control/CloudFront
aws-foundational-security-best-/1.0. practices/v 0/CloudFront.10	sicurezza- .10 control/CloudFront
aws-foundational-security-best-/1.0. practices/v 0/CloudFront.12	sicurezza- .12 control/CloudFront
aws-foundational-security-best-/1.0. practices/v 0/CloudTrail.1	sicurezza- 1. control/CloudTrail
aws-foundational-security-best-/1.0. practices/v 0/CloudTrail2.	sicurezza- 2. control/CloudTrail
aws-foundational-security-best-/1.0. practices/v 0/CloudTrail4.	sicurezza- 4. control/CloudTrail
aws-foundational-security-best-/1.0. practices/v 0/CloudTrail5.	sicurezza- 5. control/CloudTrail
aws-foundational-security-best-/1.0. practices/v 0/CodeBuild.1	sicurezza- 1. control/CodeBuild
aws-foundational-security-best-/1.0. practices/v 0/CodeBuild2.	sicurezza- 2. control/CodeBuild
aws-foundational-security-best-/1.0. practices/v 0/CodeBuild3.	sicurezza- 3. control/CodeBuild
aws-foundational-security-best-/1.0. practices/v 0/CodeBuild4.	sicurezza- 4. control/CodeBuild

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/Config.1	sicurezza- 1. control/Config
aws-foundational-security-best-/1.0. practices/v 0/DMS.1	sicurezza- 1. control/DMS
aws-foundational-security-best-/1.0. practices/v 0/DynamoDB.1	sicurezza- 1. control/DynamoDB
aws-foundational-security-best-/1.0. practices/v 0/DynamoDB2.	sicurezza- 2. control/DynamoDB
aws-foundational-security-best-/1.0. practices/v 0/DynamoDB3.	sicurezza- 3. control/DynamoDB
aws-foundational-security-best-/1.0. practices/v 0/EC2.1	sicurezza- 1. control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC23.	sicurezza- 3. control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC24.	sicurezza- 4. control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC26.	sicurezza- 6. control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC27.	sicurezza- 7. control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC28.	sicurezza- 8. control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC29.	sicurezza- 9. control/EC2

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/EC2.10	sicurezza- .10 control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC2.15	sicurezza- .15 control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC2.16	sicurezza- .16 control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC2.17	sicurezza- .17 control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC2.18	sicurezza- .18 control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC2.19	sicurezza- .19 control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC22.	sicurezza- 2. control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC2.20	sicurezza- .20 control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC22.1	sicurezza- .21 control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC2.23	sicurezza- .23 control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC2.24	sicurezza- .24 control/EC2
aws-foundational-security-best-/1.0. practices/v 0/EC2.25	sicurezza- .25 control/EC2

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/ECR.1	sicurezza- 1. control/ECR
aws-foundational-security-best-/1.0. practices/v 0/ECR2.	sicurezza- 2. control/ECR
aws-foundational-security-best-/1.0. practices/v 0/ECR3.	sicurezza- 3. control/ECR
aws-foundational-security-best-/1.0. practices/v 0/ECS.10	sicurezza- .10 control/ECS
aws-foundational-security-best-/1.0. practices/v 0/ECS.12	sicurezza- .12 control/ECS
aws-foundational-security-best-/1.0. practices/v 0/ECS2.	sicurezza- 2. control/ECS
aws-foundational-security-best-/1.0. practices/v 0/ECS3.	sicurezza- 3. control/ECS
aws-foundational-security-best-/1.0. practices/v 0/ECS4.	sicurezza- 4. control/ECS
aws-foundational-security-best-/1.0. practices/v 0/ECS5.	sicurezza- 5. control/ECS
aws-foundational-security-best-/1.0. practices/v 0/ECS8.	sicurezza- 8. control/ECS
aws-foundational-security-best-/1.0. practices/v 0/EFS.1	sicurezza- 1. control/EFS
aws-foundational-security-best-/1.0. practices/v 0/EFS2.	sicurezza- 2. control/EFS

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/EFS3.	sicurezza- 3. control/EFS
aws-foundational-security-best-/1.0. practices/v 0/EFS4.	sicurezza- 4. control/EFS
aws-foundational-security-best-/1.0. practices/v 0/EKS2.	sicurezza- 2. control/EKS
aws-foundational-security-best-/1.0. practices/v 0/ElasticBeanstalk.1	sicurezza- 1. control/ElasticBeanstalk
aws-foundational-security-best-/1.0. practices/v 0/ElasticBeanstalk2.	sicurezza- 2. control/ElasticBeanstalk
aws-foundational-security-best-/1.0. practices/v 0/ELBv2.1	sicurezza- 1. control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB2.	sicurezza- 2. control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB3.	sicurezza- 3. control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB4.	sicurezza- 4. control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB5.	sicurezza- 5. control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB6.	sicurezza- 6. control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB7.	sicurezza- 7. control/ELB

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/ELB8.	sicurezza- 8. control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB9.	sicurezza- 9. control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB.10	sicurezza- .10 control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB.11	sicurezza- .11 control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB.12	sicurezza- .12 control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB.13	sicurezza- .13 control/ELB
aws-foundational-security-best-/1.0. practices/v 0/ELB.14	sicurezza- .14 control/ELB
aws-foundational-security-best-/1.0. practices/v 0/EMR.1	sicurezza- 1. control/EMR
aws-foundational-security-best-/1.0. practices/v 0/ES.1	sicurezza- 1. control/ES
aws-foundational-security-best-/1.0. practices/v 0/ES2.	sicurezza- 2. control/ES
aws-foundational-security-best-/1.0. practices/v 0/ES3.	sicurezza- 3. control/ES
aws-foundational-security-best-/1.0. practices/v 0/ES4.	sicurezza- 4. control/ES

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/ES5.	sicurezza- 5. control/ES
aws-foundational-security-best-/1.0. practices/v 0/ES6.	sicurezza- 6. control/ES
aws-foundational-security-best-/1.0. practices/v 0/ES7.	sicurezza- 7. control/ES
aws-foundational-security-best-/1.0. practices/v 0/ES8.	sicurezza- 8. control/ES
aws-foundational-security-best-/1.0. practices/v 0/GuardDuty.1	sicurezza- 1. control/GuardDuty
aws-foundational-security-best-/1.0. practices/v 0/IAM.1	sicurezza- 1. control/IAM
aws-foundational-security-best-/1.0. practices/v 0/IAM2.	sicurezza- 2. control/IAM
aws-foundational-security-best-/1.0. practices/v 0/IAM2.1	sicurezza- .21 control/IAM
aws-foundational-security-best-/1.0. practices/v 0/IAM3.	sicurezza- 3. control/IAM
aws-foundational-security-best-/1.0. practices/v 0/IAM4.	sicurezza- 4. control/IAM
aws-foundational-security-best-/1.0. practices/v 0/IAM5.	sicurezza- 5. control/IAM
aws-foundational-security-best-/1.0. practices/v 0/IAM6.	sicurezza- 6. control/IAM

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/IAM7.	sicurezza- 7. control/IAM
aws-foundational-security-best-/1.0. practices/v 0/IAM8.	sicurezza- 8. control/IAM
aws-foundational-security-best-/1.0. practices/v 0/Kinesis.1	sicurezza- 1. control/Kinesis
aws-foundational-security-best-/1.0. practices/v 0/KMS.1	sicurezza- 1. control/KMS
aws-foundational-security-best-/1.0. practices/v 0/KMS2.	sicurezza- 2. control/KMS
aws-foundational-security-best-/1.0. practices/v 0/KMS3.	sicurezza- 3. control/KMS
aws-foundational-security-best-/1.0. practices/v 0/Lambda.1	sicurezza- 1. control/Lambda
aws-foundational-security-best-/1.0. practices/v 0/Lambda2.	sicurezza- 2. control/Lambda
aws-foundational-security-best-/1.0. practices/v 0/Lambda5.	sicurezza- 5. control/Lambda
aws-foundational-security-best-/1.0. practices/v 0/NetworkFirewall3.	sicurezza- 3. control/NetworkFirewall
aws-foundational-security-best-/1.0. practices/v 0/NetworkFirewall4.	sicurezza- 4. control/NetworkFirewall
aws-foundational-security-best-/1.0. practices/v 0/NetworkFirewall5.	sicurezza- 5. control/NetworkFirewall

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/NetworkFirewall6.	sicurezza- 6. control/NetworkFirewall
aws-foundational-security-best-/1.0. practices/v 0/Opensearch.1	sicurezza- 1. control/Opensearch
aws-foundational-security-best-/1.0. practices/v 0/Opensearch2.	sicurezza- 2. control/Opensearch
aws-foundational-security-best-/1.0. practices/v 0/Opensearch3.	sicurezza- 3. control/Opensearch
aws-foundational-security-best-/1.0. practices/v 0/Opensearch4.	sicurezza- 4. control/Opensearch
aws-foundational-security-best-/1.0. practices/v 0/Opensearch5.	sicurezza- 5. control/Opensearch
aws-foundational-security-best-/1.0. practices/v 0/Opensearch6.	sicurezza- 6. control/Opensearch
aws-foundational-security-best-/1.0. practices/v 0/Opensearch7.	sicurezza- 7. control/Opensearch
aws-foundational-security-best-/1.0. practices/v 0/Opensearch8.	sicurezza- 8. control/Opensearch
aws-foundational-security-best-/1.0. practices/v 0/RDS.1	sicurezza- 1. control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.10	sicurezza- .10 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.11	sicurezza- .11 control/RDS

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/RDS.12	sicurezza- .12 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.13	sicurezza- .13 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.14	sicurezza- .14 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.15	sicurezza- .15 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.16	sicurezza- .16 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.17	sicurezza- .17 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.19	sicurezza- .19 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS2.	sicurezza- 2. control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.20	sicurezza- .20 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS2.1	sicurezza- .21 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.22	sicurezza- .22 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.23	sicurezza- .23 control/RDS

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/RDS.24	sicurezza- .24 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS.25	sicurezza- .25 control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS3.	sicurezza- 3. control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS4.	sicurezza- 4. control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS5.	sicurezza- 5. control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS6.	sicurezza- 6. control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS7.	sicurezza- 7. control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS8.	sicurezza- 8. control/RDS
aws-foundational-security-best-/1.0. practices/v 0/RDS9.	sicurezza- 9. control/RDS
aws-foundational-security-best-/1.0. practices/v 0/Redshift.1	sicurezza- 1. control/Redshift
aws-foundational-security-best-/1.0. practices/v 0/Redshift2.	sicurezza- 2. control/Redshift
aws-foundational-security-best-/1.0. practices/v 0/Redshift3.	sicurezza- 3. control/Redshift

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/Redshift4.	sicurezza- 4. control/Redshift
aws-foundational-security-best-/1.0. practices/v 0/Redshift6.	sicurezza- 6. control/Redshift
aws-foundational-security-best-/1.0. practices/v 0/Redshift7.	sicurezza- 7. control/Redshift
aws-foundational-security-best-/1.0. practices/v 0/Redshift8.	sicurezza- 8. control/Redshift
aws-foundational-security-best-/1.0. practices/v 0/S3.1	sicurezza- 1. control/S3
aws-foundational-security-best-/1.0. practices/v 0/S3.12	sicurezza- .12 control/S3
aws-foundational-security-best-/1.0. practices/v 0/S3.13	sicurezza- .13 control/S3
aws-foundational-security-best-/1.0. practices/v 0/S32.	sicurezza- 2. control/S3
aws-foundational-security-best-/1.0. practices/v 0/S33.	sicurezza- 3. control/S3
aws-foundational-security-best-/1.0. practices/v 0/S35.	sicurezza- 5. control/S3
aws-foundational-security-best-/1.0. practices/v 0/S36.	sicurezza- 6. control/S3
aws-foundational-security-best-/1.0. practices/v 0/S38.	sicurezza- 8. control/S3

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/S39.	sicurezza- 9. control/S3
aws-foundational-security-best-/1.0. practices/v 0/SageMaker.1	sicurezza- 1. control/SageMaker
aws-foundational-security-best-/1.0. practices/v 0/SageMaker2.	sicurezza- 2. control/SageMaker
aws-foundational-security-best-/1.0. practices/v 0/SageMaker3.	sicurezza- 3. control/SageMaker
aws-foundational-security-best-/1.0. practices/v 0/SecretsManager.1	sicurezza- 1. control/SecretsManager
aws-foundational-security-best-/1.0. practices/v 0/SecretsManager2.	sicurezza- 2. control/SecretsManager
aws-foundational-security-best-/1.0. practices/v 0/SecretsManager3.	sicurezza- 3. control/SecretsManager
aws-foundational-security-best-/1.0. practices/v 0/SecretsManager4.	sicurezza- 4. control/SecretsManager
aws-foundational-security-best-/1.0. practices/v 0/SQS.1	sicurezza- 1. control/SQS
aws-foundational-security-best-/1.0. practices/v 0/SSM.1	sicurezza- 1. control/SSM
aws-foundational-security-best-/1.0. practices/v 0/SSM2.	sicurezza- 2. control/SSM
aws-foundational-security-best-/1.0. practices/v 0/SSM3.	sicurezza- 3. control/SSM

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
aws-foundational-security-best-/1.0. practices/v 0/SSM4.	sicurezza- 4. control/SSM
aws-foundational-security-best-/1.0. practices/v 0/WAF.1	sicurezza- 1. control/WAF
aws-foundational-security-best-/1.0. practices/v 0/WAF2.	sicurezza- 2. control/WAF
aws-foundational-security-best-/1.0. practices/v 0/WAF3.	sicurezza- 3. control/WAF
aws-foundational-security-best-/1.0. practices/v 0/WAF4.	sicurezza- 4. control/WAF
aws-foundational-security-best-/1.0. practices/v 0/WAF6.	sicurezza- 6. control/WAF
aws-foundational-security-best-/1.0. practices/v 0/WAF7.	sicurezza- 7. control/WAF
aws-foundational-security-best-/1.0. practices/v 0/WAF8.	sicurezza- 8. control/WAF
aws-foundational-security-best-/1.0. practices/v 0/WAF.10	sicurezza- .10 control/WAF
pci- /3.2. dss/v 1/PCI. AutoScaling.1	sicurezza- 1control/AutoScaling.
pci- /3.2. dss/v 1/PCI. CloudTrail.1	sicurezza- 2control/CloudTrail.
pci- /3.2. dss/v 1/PCI. CloudTrail.2	sicurezza- 3control/CloudTrail.
pci- /3.2. dss/v 1/PCI. CloudTrail.3	sicurezza- 4control/CloudTrail.
pci- /3.2. dss/v 1/PCI. CloudTrail.4	sicurezza- 5control/CloudTrail.

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
pci- /3.2. dss/v 1/PCI. CodeBuild.1	sicurezza- 1control/CodeBuild.
pci- /3.2. dss/v 1/PCI. CodeBuild.2	sicurezza- 2control/CodeBuild.
pci- /3.2. dss/v 1/PCI. Config.1	sicurezza- 1control/Config.
pci- /3.2. dss/v 1/PCI. CW.1	sicurezza- 1control/CloudWatch.
pci- /3.2. dss/v 1/PCI. DMS.1	sicurezza- 1control/DMS.
pci- /3.2. dss/v 1/PCI. EC2.1	sicurezza- 1control/EC2.
pci- /3.2. dss/v 1/PCI. EC2.2	sicurezza- 2control/EC2.
pci- /3.2. dss/v 1/PCI. EC2.4	sicurezza- control/EC2 1.2
pci- /3.2. dss/v 1/PCI. EC2.5	sicurezza- control/EC2 1.3
pci- /3.2. dss/v 1/PCI. EC2.6	sicurezza- 6control/EC2.
pci- /3.2. dss/v 1/PCI. ELBv2.1	sicurezza- 1control/ELB.
pci- /3.2. dss/v 1/PCI. ES.1	sicurezza- 2control/ES.
pci- /3.2. dss/v 1/PCI. ES.2	sicurezza- 1control/ES.
pci- /3.2. dss/v 1/PCI. GuardDuty.1	sicurezza- 1control/GuardDuty.
pci- /3.2. dss/v 1/PCI. IAM.1	sicurezza- 4control/IAM.
pci- /3.2. dss/v 1/PCI. IAM.2	sicurezza- 2control/IAM.
pci- /3.2. dss/v 1/PCI. IAM.3	sicurezza- 1control/IAM.
pci- /3.2. dss/v 1/PCI. IAM.4	sicurezza- 6control/IAM.
pci- /3.2. dss/v 1/PCI. IAM.5	sicurezza- 9control/IAM.
pci- /3.2. dss/v 1/PCI. IAM.6	sicurezza- control/IAM 1.9

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
pci- /3.2. dss/v 1/PCI. IAM.7	sicurezza- 8control/IAM.
pci- /3.2. dss/v 1/PCI. IAM.8	sicurezza- control/IAM 1.0
pci- /3.2. dss/v 1/PCI. KMS.1	sicurezza- 4control/KMS.
pci- /3.2. dss/v 1/PCI. Lambda.1	sicurezza- 1control/Lambda.
pci- /3.2. dss/v 1/PCI. Lambda.2	sicurezza- 3control/Lambda.
pci- /3.2. dss/v 1/PCI. Opensearch.1	sicurezza- 2control/Opensearch.
pci- /3.2. dss/v 1/PCI. Opensearch.2	sicurezza- 1control/Opensearch.
pci- /3.2. dss/v 1/PCI. RDS.1	sicurezza- 1control/RDS.
pci- /3.2. dss/v 1/PCI. RDS.2	sicurezza- 2control/RDS.
pci- /3.2. dss/v 1/PCI. Redshift.1	sicurezza- 1control/Redshift.
pci- /3.2. dss/v 1/PCI. S3.1	sicurezza- 3control/S3.
pci- /3.2. dss/v 1/PCI. S3.2	sicurezza- 2control/S3.
pci- /3.2. dss/v 1/PCI. S3.3	sicurezza- 7control/S3.
pci- /3.2. dss/v 1/PCI. S3.5	sicurezza- 5control/S3.
pci- /3.2. dss/v 1/PCI. S3.6	sicurezza- 1control/S3.
pci- /3.2. dss/v 1/PCI. SageMaker.1	sicurezza- 1control/SageMaker.
pci- /3.2. dss/v 1/PCI. SSM.1	sicurezza- 2control/SSM.
pci- /3.2. dss/v 1/PCI. SSM.2	sicurezza- 3control/SSM.
pci- /3.2. dss/v 1/PCI. SSM.3	sicurezza- 1control/SSM.

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
servizio gestito-aws-control- /1.0. tower/v 0/ ACM.1	sicurezza- 1. control/ACM
servizio gestito-aws-control- /1.0. tower/v 0/ APIGateway.1	sicurezza- 1. control/APIGateway
servizio gestito-aws-control- /1.0. tower/v 0/ APIGateway2.	sicurezza- 2. control/APIGateway
gestione del servizio aws-control- /1.0. tower/v 0/APIGateway3.	sicurezza- 3. control/APIGateway
gestione del servizio aws-control- /1.0. tower/v 0/APIGateway4.	sicurezza- 4. control/APIGateway
servizio gestito-aws-control- /1.0. tower/v 0/ APIGateway5.	sicurezza- 5. control/APIGateway
servizio gestito-aws-control- /1.0. tower/v 0/ AutoScaling.1	sicurezza- 1. control/AutoScaling
servizio gestito-aws-control- /1.0. tower/v 0/ AutoScaling2.	sicurezza- 2. control/AutoScaling
gestione del servizio aws-control- /1.0. tower/v 0/AutoScaling3.	sicurezza- 3. control/AutoScaling
gestione del servizio aws-control- /1.0. tower/v 0/AutoScaling4.	sicurezza- 4. control/AutoScaling
servizio gestito-aws-control- /1.0. tower/v 0/ Autoscaling5.	sicurezza- 5. control/Autoscaling
servizio gestito-aws-control- /1.0. tower/v 0/ AutoScaling6.	sicurezza- 6. control/AutoScaling

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
servizio gestito-aws-control- /1.0. tower/v 0/ AutoScaling9.	sicurezza- 9. control/AutoScaling
servizio gestito-aws-control- /1.0. tower/v 0/ CloudTrail.1	sicurezza- 1. control/CloudTrail
servizio gestito-aws-control- /1.0. tower/v 0/ CloudTrail2.	sicurezza- 2. control/CloudTrail
gestione del servizio aws-control- /1.0. tower/v 0/CloudTrail4.	sicurezza- 4. control/CloudTrail
servizio gestito-aws-control- /1.0. tower/v 0/ CloudTrail5.	sicurezza- 5. control/CloudTrail
servizio gestito-aws-control- /1.0. tower/v 0/ CodeBuild.1	sicurezza- 1. control/CodeBuild
servizio gestito-aws-control- /1.0. tower/v 0/ CodeBuild2.	sicurezza- 2. control/CodeBuild
gestione del servizio aws-control- /1.0. tower/v 0/CodeBuild4.	sicurezza- 4. control/CodeBuild
servizio gestito-aws-control- /1.0. tower/v 0/ DMS.1	sicurezza- 1. control/DMS
servizio gestito-aws-control- /1.0. tower/v 0/ DynamoDB.1	sicurezza- 1. control/DynamoDB
servizio gestito-aws-control- /1.0. tower/v 0/ DynamoDB2.	sicurezza- 2. control/DynamoDB
gestione del servizio aws-control- /1.0. tower/v 0/EC2.1	sicurezza- 1. control/EC2

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
servizio gestito-aws-control- /1.0. tower/v 0/ EC22.	sicurezza- 2. control/EC2
gestione del servizio aws-control- /1.0. tower/v 0/EC23.	sicurezza- 3. control/EC2
gestione del servizio aws-control- /1.0. tower/v 0/EC24.	sicurezza- 4. control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC26.	sicurezza- 6. control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC27.	sicurezza- 7. control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC28.	sicurezza- 8. control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC29.	sicurezza- 9. control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC2.10	sicurezza- .10 control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC2.15	sicurezza- .15 control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC2.16	sicurezza- .16 control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC2.17	sicurezza- .17 control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC2.18	sicurezza- .18 control/EC2

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
servizio gestito-aws-control- /1.0. tower/v 0/ EC2.19	sicurezza- .19 control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC2.20	sicurezza- .20 control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC22.1	sicurezza- .21 control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ EC2.22	sicurezza- .22 control/EC2
servizio gestito-aws-control- /1.0. tower/v 0/ ECR.1	sicurezza- 1. control/ECR
servizio gestito-aws-control- /1.0. tower/v 0/ ECR2.	sicurezza- 2. control/ECR
gestione del servizio aws-control- /1.0. tower/v 0/ECR3.	sicurezza- 3. control/ECR
gestione del servizio aws-control- /1.0. tower/v 0/ECS2.	sicurezza- 2. control/ECS
gestione del servizio aws-control- /1.0. tower/v 0/ECS3.	sicurezza- 3. control/ECS
gestione del servizio aws-control- /1.0. tower/v 0/ECS4.	sicurezza- 4. control/ECS
servizio gestito-aws-control- /1.0. tower/v 0/ ECS5.	sicurezza- 5. control/ECS
servizio gestito-aws-control- /1.0. tower/v 0/ ECS8.	sicurezza- 8. control/ECS

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
servizio gestito-aws-control- /1.0. tower/v 0/ ECS.10	sicurezza- .10 control/ECS
servizio gestito-aws-control- /1.0. tower/v 0/ ECS.12	sicurezza- .12 control/ECS
servizio gestito-aws-control- /1.0. tower/v 0/ EFS.1	sicurezza- 1. control/EFS
servizio gestito-aws-control- /1.0. tower/v 0/ EFS2.	sicurezza- 2. control/EFS
gestione del servizio aws-control- /1.0. tower/v 0/EFS3.	sicurezza- 3. control/EFS
gestione del servizio aws-control- /1.0. tower/v 0/EFS4.	sicurezza- 4. control/EFS
servizio gestito-aws-control- /1.0. tower/v 0/ EKS2.	sicurezza- 2. control/EKS
gestione del servizio aws-control- /1.0. tower/v 0/ELB2.	sicurezza- 2. control/ELB
gestione del servizio aws-control- /1.0. tower/v 0/ELB3.	sicurezza- 3. control/ELB
gestione del servizio aws-control- /1.0. tower/v 0/ELB4.	sicurezza- 4. control/ELB
servizio gestito-aws-control- /1.0. tower/v 0/ ELB5.	sicurezza- 5. control/ELB
servizio gestito-aws-control- /1.0. tower/v 0/ ELB6.	sicurezza- 6. control/ELB

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
servizio gestito-aws-control- /1.0. tower/v 0/ ELB7.	sicurezza- 7. control/ELB
servizio gestito-aws-control- /1.0. tower/v 0/ ELB8.	sicurezza- 8. control/ELB
servizio gestito-aws-control- /1.0. tower/v 0/ ELB9.	sicurezza- 9. control/ELB
servizio gestito-aws-control- /1.0. tower/v 0/ ELB.10	sicurezza- .10 control/ELB
servizio gestito-aws-control- /1.0. tower/v 0/ ELB.12	sicurezza- .12 control/ELB
servizio gestito-aws-control- /1.0. tower/v 0/ ELB.13	sicurezza- .13 control/ELB
servizio gestito-aws-control- /1.0. tower/v 0/ ELB.14	sicurezza- .14 control/ELB
servizio gestito-aws-control- /1.0. tower/v 0/ ELBv2.1	sicurezza- 1. control/ELBv2
servizio gestito-aws-control- /1.0. tower/v 0/ EMR.1	sicurezza- 1. control/EMR
servizio gestito-aws-control- /1.0. tower/v 0/ ES.1	sicurezza- 1. control/ES
servizio gestito-aws-control- /1.0. tower/v 0/ ES2.	sicurezza- 2. control/ES
gestione del servizio aws-control- /1.0. tower/v 0/ES3.	sicurezza- 3. control/ES

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
gestione del servizio aws-control- /1.0. tower/v 0/ES4.	sicurezza- 4. control/ES
servizio gestito-aws-control- /1.0. tower/v 0/ ES5.	sicurezza- 5. control/ES
servizio gestito-aws-control- /1.0. tower/v 0/ ES6.	sicurezza- 6. control/ES
servizio gestito-aws-control- /1.0. tower/v 0/ ES7.	sicurezza- 7. control/ES
servizio gestito-aws-control- /1.0. tower/v 0/ ES8.	sicurezza- 8. control/ES
servizio gestito-aws-control- /1.0. tower/v 0/ ElasticBeanstalk.1	sicurezza- 1. control/ElasticBeanstalk
servizio gestito-aws-control- /1.0. tower/v 0/ ElasticBeanstalk2.	sicurezza- 2. control/ElasticBeanstalk
gestione del servizio aws-control- /1.0. tower/v 0/GuardDuty.1	sicurezza- 1. control/GuardDuty
servizio gestito-aws-control- /1.0. tower/v 0/ IAM.1	sicurezza- 1. control/IAM
servizio gestito-aws-control- /1.0. tower/v 0/ IAM2.	sicurezza- 2. control/IAM
gestione del servizio aws-control- /1.0. tower/v 0/IAM3.	sicurezza- 3. control/IAM
gestione del servizio aws-control- /1.0. tower/v 0/IAM4.	sicurezza- 4. control/IAM

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
servizio gestito-aws-control- /1.0. tower/v 0/ IAM5.	sicurezza- 5. control/IAM
servizio gestito-aws-control- /1.0. tower/v 0/ IAM6.	sicurezza- 6. control/IAM
servizio gestito-aws-control- /1.0. tower/v 0/ IAM7.	sicurezza- 7. control/IAM
servizio gestito-aws-control- /1.0. tower/v 0/ IAM8.	sicurezza- 8. control/IAM
servizio gestito-aws-control- /1.0. tower/v 0/ IAM2.1	sicurezza- .21 control/IAM
servizio gestito-aws-control- /1.0. tower/v 0/ Kinesis.1	sicurezza- 1. control/Kinesis
servizio gestito-aws-control- /1.0. tower/v 0/ KMS.1	sicurezza- 1. control/KMS
servizio gestito-aws-control- /1.0. tower/v 0/ KMS2.	sicurezza- 2. control/KMS
gestione del servizio aws-control- /1.0. tower/v 0/KMS3.	sicurezza- 3. control/KMS
gestione del servizio aws-control- /1.0. tower/v 0/Lambda.1	sicurezza- 1. control/Lambda
servizio gestito-aws-control- /1.0. tower/v 0/ Lambda2.	sicurezza- 2. control/Lambda
gestione del servizio aws-control- /1.0. tower/v 0/Lambda5.	sicurezza- 5. control/Lambda

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
servizio gestito-aws-control- /1.0. tower/v 0/ NetworkFirewall3.	sicurezza- 3. control/NetworkFirewall
gestione del servizio aws-control- /1.0. tower/v 0/NetworkFirewall4.	sicurezza- 4. control/NetworkFirewall
servizio gestito-aws-control- /1.0. tower/v 0/ NetworkFirewall5.	sicurezza- 5. control/NetworkFirewall
servizio gestito-aws-control- /1.0. tower/v 0/ NetworkFirewall6.	sicurezza- 6. control/NetworkFirewall
servizio gestito-aws-control- /1.0. tower/v 0/ Opensearch.1	sicurezza- 1. control/Opensearch
servizio gestito-aws-control- /1.0. tower/v 0/ Opensearch2.	sicurezza- 2. control/Opensearch
gestione del servizio aws-control- /1.0. tower/v 0/Opensearch3.	sicurezza- 3. control/Opensearch
gestione del servizio aws-control- /1.0. tower/v 0/Opensearch4.	sicurezza- 4. control/Opensearch
servizio gestito-aws-control- /1.0. tower/v 0/ Opensearch5.	sicurezza- 5. control/Opensearch
servizio gestito-aws-control- /1.0. tower/v 0/ Opensearch6.	sicurezza- 6. control/Opensearch
servizio gestito-aws-control- /1.0. tower/v 0/ Opensearch7.	sicurezza- 7. control/Opensearch
servizio gestito-aws-control- /1.0. tower/v 0/ Opensearch8.	sicurezza- 8. control/Opensearch

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
servizio gestito-aws-control- /1.0. tower/v 0/ RDS.1	sicurezza- 1. control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS2.	sicurezza- 2. control/RDS
gestione del servizio aws-control- /1.0. tower/v 0/RDS3.	sicurezza- 3. control/RDS
gestione del servizio aws-control- /1.0. tower/v 0/RDS4.	sicurezza- 4. control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS5.	sicurezza- 5. control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS6.	sicurezza- 6. control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS8.	sicurezza- 8. control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS9.	sicurezza- 9. control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS.10	sicurezza- .10 control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS.11	sicurezza- .11 control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS.13	sicurezza- .13 control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS.17	sicurezza- .17 control/RDS

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
servizio gestito-aws-control- /1.0. tower/v 0/ RDS.19	sicurezza- .19 control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS.20	sicurezza- .20 control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS2.1	sicurezza- .21 control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS.22	sicurezza- .22 control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS.23	sicurezza- .23 control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ RDS.25	sicurezza- .25 control/RDS
servizio gestito-aws-control- /1.0. tower/v 0/ Redshift.1	sicurezza- 1. control/Redshift
servizio gestito-aws-control- /1.0. tower/v 0/ Redshift2.	sicurezza- 2. control/Redshift
gestione del servizio aws-control- /1.0. tower/v 0/Redshift4.	sicurezza- 4. control/Redshift
servizio gestito-aws-control- /1.0. tower/v 0/ Redshift6.	sicurezza- 6. control/Redshift
servizio gestito-aws-control- /1.0. tower/v 0/ Redshift7.	sicurezza- 7. control/Redshift
servizio gestito-aws-control- /1.0. tower/v 0/ Redshift8.	sicurezza- 8. control/Redshift

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
servizio gestito-aws-control- /1.0. tower/v 0/ S3.1	sicurezza- 1. control/S3
servizio gestito-aws-control- /1.0. tower/v 0/ S32.	sicurezza- 2. control/S3
gestione del servizio aws-control- /1.0. tower/v 0/S33.	sicurezza- 3. control/S3
gestione del servizio aws-control- /1.0. tower/v 0/S35.	sicurezza- 5. control/S3
servizio gestito-aws-control- /1.0. tower/v 0/ S36.	sicurezza- 6. control/S3
servizio gestito-aws-control- /1.0. tower/v 0/ S38.	sicurezza- 8. control/S3
servizio gestito-aws-control- /1.0. tower/v 0/ S39.	sicurezza- 9. control/S3
servizio gestito-aws-control- /1.0. tower/v 0/ S3.12	sicurezza- .12 control/S3
servizio gestito-aws-control- /1.0. tower/v 0/ S3.13	sicurezza- .13 control/S3
servizio gestito-aws-control- /1.0. tower/v 0/ SageMaker.1	sicurezza- 1. control/SageMaker
servizio gestito-aws-control- /1.0. tower/v 0/ SecretsManager.1	sicurezza- 1. control/SecretsManager
servizio gestito-aws-control- /1.0. tower/v 0/ SecretsManager2.	sicurezza- 2. control/SecretsManager

GeneratorID prima di abilitare i risultati di controllo consolidati	GeneratorID dopo aver abilitato i risultati di controllo consolidati
gestione del servizio aws-control- /1.0. tower/v 0/SecretsManager3.	sicurezza- 3. control/SecretsManager
gestione del servizio aws-control- /1.0. tower/v 0/SecretsManager4.	sicurezza- 4. control/SecretsManager
servizio gestito-aws-control- /1.0. tower/v 0/ SQS.1	sicurezza- 1. control/SQS
servizio gestito-aws-control- /1.0. tower/v 0/ SSM.1	sicurezza- 1. control/SSM
servizio gestito-aws-control- /1.0. tower/v 0/ SSM2.	sicurezza- 2. control/SSM
gestione del servizio aws-control- /1.0. tower/v 0/SSM3.	sicurezza- 3. control/SSM
gestione del servizio aws-control- /1.0. tower/v 0/SSM4.	sicurezza- 4. control/SSM
servizio gestito-aws-control- /1.0. tower/v 0/ WAF2.	sicurezza- 2. control/WAF
gestione del servizio aws-control- /1.0. tower/v 0/WAF3.	sicurezza- 3. control/WAF
gestione del servizio aws-control- /1.0. tower/v 0/WAF4.	sicurezza- 4. control/WAF

In che modo il consolidamento influisce sugli ID e sui titoli di controllo

Controlli consolidati La visualizzazione e i risultati dei controlli consolidati standardizzano gli ID e i titoli di controllo in tutti gli standard. I termini Security Control ID e Security Control Title si riferiscono a questi valori indipendenti dallo standard.

La console Security Hub CSPM mostra ID di controllo di sicurezza e titoli di controllo di sicurezza indipendenti dagli standard, indipendentemente dal fatto che i risultati del controllo consolidato siano abilitati o disabilitati per l'account. Tuttavia, i risultati CSPM di Security Hub contengono titoli di controllo specifici per PCI DSS e CIS v1.2.0, se i risultati del controllo consolidato sono disabilitati per l'account. Inoltre, i risultati CSPM di Security Hub contengono l'ID di controllo e l'ID di controllo di sicurezza specifici dello standard. Per esempi di come il consolidamento influisce sui risultati del controllo, vedi. Esempi di risultati di controllo

Per i controlli che fanno parte dello standard AWS Control Tower gestito dai servizi, il prefisso `CT.` viene rimosso dall'ID del controllo e dal titolo nei risultati quando i risultati del controllo consolidato sono abilitati.

Per disabilitare un controllo di sicurezza in Security Hub CSPM, è necessario disabilitare tutti i controlli standard che corrispondono al controllo di sicurezza. La tabella seguente mostra la mappatura degli ID e dei titoli dei controlli di sicurezza agli ID e ai titoli di controllo specifici dello standard. Gli ID e i titoli dei controlli che appartengono allo standard AWS Foundational Security Best Practices (FSBP) sono già indipendenti dallo standard. Per una mappatura dei controlli ai requisiti di Center for Internet Security (CIS) v3.0.0, vedere. Mappatura dei controlli in base ai requisiti CIS in ogni versione Per eseguire i propri script su questa tabella, è possibile scaricarla come file.csv.

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	1.1 Evita l'uso dell'utente root	[CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»
CIS versione 1.2.0	1.10 Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password	[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
CIS versione 1.2.0	1.11 Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno	[IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno
CIS versione 1.2.0	1.12 Assicurati che non esista alcuna chiave di accesso per l'utente root	[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	1.13 Assicurarsi che l'MFA sia abilitata per l'utente root	[IAM.9] L'MFA deve essere abilitata per l'utente root
CIS versione 1.2.0	1.14 Assicurarsi che l'MFA hardware sia abilitato per l'utente root	[IAM.6] La MFA hardware deve essere abilitata per l'utente root
CIS versione 1.2.0	1.16 Assicurati che le policy IAM siano collegate solo a gruppi o ruoli	[IAM.2] Gli utenti IAM non devono avere policy IAM allegate
CIS versione 1.2.0	1.2 Assicurati che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti IAM che dispongono di una password di console	[IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
CIS versione 1.2.0	1.20 Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto	[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
CIS versione 1.2.0	1.22 Assicurati che non vengano create politiche IAM che consentano privilegi amministrativi completi «*: *»	[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
CIS versione 1.2.0	1.3 Assicurati che le credenziali non utilizzate per 90 giorni o più siano disabilitate	[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
CIS versione 1.2.0	1.4 Assicurati che le chiavi di accesso vengano ruotate ogni 90 giorni o meno	[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
CIS versione 1.2.0	1.5 Assicurati che la politica delle password di IAM richieda almeno una lettera maiuscola	[IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	1.6 Assicurati che la politica delle password di IAM richieda almeno una lettera minuscola	[IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
CIS versione 1.2.0	1.7 Assicurati che la politica delle password IAM richieda almeno un simbolo	[IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
CIS versione 1.2.0	1.8 Assicurati che la politica delle password IAM richieda almeno un numero	[IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
CIS versione 1.2.0	1.9 Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14	[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
CIS versione 1.2.0	2.1 Ensure CloudTrail è abilitato in tutte le regioni	[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura
CIS versione 1.2.0	2.2 Assicurarsi che la convalida dei file di CloudTrail registro sia abilitata	[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata
CIS versione 1.2.0	2.3 Assicurati che il bucket S3 utilizzato per archiviare CloudTrail i log non sia accessibile al pubblico	[CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico
CIS versione 1.2.0	2.4 Assicurati che i CloudTrail percorsi siano integrati con i log CloudWatch	[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	2.5 Assicurati che AWS Config sia abilitato	[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse
CIS versione 1.2.0	2.6 Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail	[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
CIS versione 1.2.0	2.7 Assicurati che i CloudTrail log siano crittografati quando sono inattivi utilizzando le CMK KMS	[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata
CIS versione 1.2.0	2.8 Assicurati che la rotazione per le CMK create dal cliente sia abilitata	[KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata
CIS versione 1.2.0	2.9 Assicurati che la registrazione del flusso VPC sia abilitata in tutti i VPC	[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC
CIS versione 1.2.0	3.1 Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate	[CloudWatch.2] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate
CIS versione 1.2.0	3.10 Assicurarsi che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza	[CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza
CIS versione 1.2.0	3.11 Assicurarsi che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)	[CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	3.12 Assicurarsi che esistano un filtro metrico di registro e un allarme per le modifiche ai gateway di rete	[CloudWatch.12] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gateway di rete
CIS versione 1.2.0	3.13 Assicurarsi che esistano un filtro metrico di log e un allarme per le modifiche alla tabella di percorso	[CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte
CIS versione 1.2.0	3.14 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche al VPC	[CloudWatch.14] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche al VPC
CIS versione 1.2.0	3.2 Assicurarsi che esistano un filtro metrico di registro e un allarme per l'accesso alla Console di gestione senza MFA	[CloudWatch.3] Assicurati che esistano un filtro metrico di registro e un allarme per l'accesso alla console di gestione senza MFA
CIS versione 1.2.0	3.3 Assicurarsi che esistano un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente root	[CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»
CIS versione 1.2.0	3.4 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle politiche IAM	[CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM
CIS versione 1.2.0	3.5 Assicurati che esistano un filtro metrico di registro e un allarme per le CloudTrail modifiche alla configurazione	[CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrail alla configurazione

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	3.6 Assicurati che esistano un filtro metrico di registro e un allarme per gli errori di autenticazione Console di gestione AWS	[CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per Console di gestione AWS errori di autenticazione
CIS versione 1.2.0	3.7 Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione pianificata delle CMK create dal cliente	[CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione pianificata delle chiavi gestite dal cliente
CIS versione 1.2.0	3.8 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy relative ai bucket S3	[CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3
CIS versione 1.2.0	3.9 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla configurazione AWS Config	[CloudWatch.9] Assicurati che esistano un filtro metrico di registro e un allarme per AWS Config modifiche alla configurazione
CIS versione 1.2.0	4.1 Assicurarsi che nessun gruppo di sicurezza consenta l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22	[EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22
CIS versione 1.2.0	4.2 Assicurarsi che nessun gruppo di sicurezza consenta l'ingresso da 0.0.0. 0/0 alla porta 3389	[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
CIS versione 1.2.0	4.3 Assicurati che il gruppo di sicurezza predefinito di ogni VPC limiti tutto il traffico	[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.4.0	1.10 Assicurati che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti IAM che dispongono di una password di console	[IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
CIS versione 1.4.0	1.14 Assicurati che le chiavi di accesso vengano ruotate ogni 90 giorni o meno	[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
CIS versione 1.4.0	1.16 Assicurati che le politiche IAM che consentono i privilegi amministrativi «*: *» completi non siano allegate	[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
CIS versione 1.4.0	1.17 Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto	[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
CIS versione 1.4.0	1.4 Assicurati che non esista alcuna chiave di accesso all'account utente root	[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
CIS versione 1.4.0	1.5 Assicurarsi che l'MFA sia abilitata per l'account utente root	[IAM.9] L'MFA deve essere abilitata per l'utente root
CIS versione 1.4.0	1.6 Assicurarsi che l'MFA hardware sia abilitata per l'account utente root	[IAM.6] La MFA hardware deve essere abilitata per l'utente root
CIS versione 1.4.0	1.7 Eliminare l'uso dell'utente root per le attività amministrative e quotidiane	[CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.4.0	1.8 Assicurati che la politica delle password IAM richieda una lunghezza minima di 14 o superiore	[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
CIS versione 1.4.0	1.9 Assicurati che la politica delle password IAM impedisca il riutilizzo delle password	[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
CIS versione 1.4.0	2.1.2 Assicurati che S3 Bucket Policy sia impostata per negare le richieste HTTP	[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS
CIS versione 1.4.0	2.1.5.1 L'impostazione S3 Block Public Access deve essere abilitata	[S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate
CIS versione 1.4.0	2.1.5.2 L'impostazione S3 Block Public Access deve essere abilitata a livello di bucket	[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico
CIS versione 1.4.0	2.2.1 Assicurarsi che la crittografia dei volumi EBS sia abilitata	[EC2.7] La crittografia predefinita di EBS deve essere abilitata
CIS versione 1.4.0	2.3.1 Assicurarsi che la crittografia sia abilitata per le istanze RDS	[RDS.3] Le istanze DB RDS devono avere la crittografia a riposo abilitata
CIS versione 1.4.0	3.1 Ensure CloudTrail è abilitato in tutte le regioni	[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura
CIS versione 1.4.0	3.2 Assicurarsi che la convalida dei file di CloudTrail registro sia abilitata	[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.4.0	3.4 Assicurati che i CloudTrail percorsi siano integrati con i registri CloudWatch	[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs
CIS versione 1.4.0	3.5 Ensure AWS Config è abilitato in tutte le regioni	[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse
CIS versione 1.4.0	3.6 Assicurati che la registraz ione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail	[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
CIS versione 1.4.0	3.7 Assicurati che i CloudTrail log siano crittografati quando sono inattivi utilizzando le CMK KMS	[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata
CIS versione 1.4.0	3.8 Assicurati che la rotazione per le CMK create dal cliente sia abilitata	[KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata
CIS versione 1.4.0	3.9 Assicurati che la registrazione del flusso VPC sia abilitata in tutti i VPC	[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC
CIS versione 1.4.0	4.4 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM	[CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM
CIS versione 1.4.0	4.5 Assicurarsi che esistano un filtro metrico di log e un allarme per le modifiche alla configurazione CloudTrail	[CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrai l alla configurazione

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.4.0	4.6 Assicurarsi che esistano un filtro metrico di registro e un allarme per gli errori di autenticazione Console di gestione AWS	[CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per Console di gestione AWS errori di autenticazione
CIS versione 1.4.0	4.7 Assicurati che esistano un filtro metrico di log e un allarme per la disabilitazione o l'eliminazione pianificata delle CMK create dal cliente	[CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione pianificata delle chiavi gestite dal cliente
CIS versione 1.4.0	4.8 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla policy dei bucket S3	[CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3
CIS versione 1.4.0	4.9 Assicurarsi che esistano un filtro metrico di log e un allarme per le modifiche alla configurazione AWS Config	[CloudWatch.9] Assicurati che esistano un filtro metrico di registro e un allarme per AWS Config modifiche alla configurazione
CIS versione 1.4.0	4.10 Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza	[CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza
CIS versione 1.4.0	4.11 Assicurarsi che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)	[CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)
CIS versione 1.4.0	4.12 Assicurarsi che esistano un filtro metrico di log e un allarme per le modifiche ai gateway di rete	[CloudWatch.12] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gateway di rete

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.4.0	4.13 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte	[CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte
CIS versione 1.4.0	4.14 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche al VPC	[CloudWatch.14] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche al VPC
CIS versione 1.4.0	5.1 Assicurarsi che nessun ACL di rete consenta l'ingresso dalla versione 0.0.0. 0/0 alle porte di amministrazione del server remoto	[EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
CIS versione 1.4.0	5.3 Assicurati che il gruppo di sicurezza predefinito di ogni VPC limiti tutto il traffico	[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita
PCI DSS v3.2.1	PCI.AutoScaling.1 I gruppi di scalabilità automatica associati a un sistema di bilanciamento del carico devono utilizzare i controlli dello stato del sistema di bilanciamento del carico	[AutoScaling.1] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB
PCI DSS v3.2.1	PCI.CloudTrail.1 CloudTrail i log devono essere crittografati quando sono inattivi utilizzando CMK AWS KMS	[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata
PCI DSS v3.2.1	PCI.CloudTrail.2 CloudTrail dovrebbe essere abilitato	[CloudTrail.3] Almeno un CloudTrail percorso deve essere abilitato
PCI DSS v3.2.1	PCI.CloudTrail.3 CloudTrail la convalida dei file di registro deve essere abilitata	[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
PCI DSS v3.2.1	PCI.CloudTrail.4 CloudTrail i trail devono essere integrati con Amazon CloudWatch Logs	[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon CloudWatch Logs
PCI DSS v3.2.1	PCI.CodeBuild.1 CodeBuild GitHub oppure gli URL del repository di origine Bitbucket devono utilizzare OAuth	[CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili
PCI DSS v3.2.1	PCI.CodeBuild.2 CodeBuild le variabili di ambiente del progetto non devono contenere credenziali di testo non crittografato	[CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato
PCI DSS v3.2.1	PCI.Config.1 AWS Config dovrebbe essere abilitato	[Config.1] AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse
PCI DSS v3.2.1	PCI.CW.1 Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»	[CloudWatch.1] Dovrebbero esistere un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»
PCI DSS v3.2.1	PCI.DMS.1 Le istanze di replica del Database Migration Service non devono essere pubbliche	[DMS.1] Le istanze di replica del Database Migration Service non devono essere pubbliche
PCI DSS v3.2.1	PCI.EC2.1 Le istantanee EBS non devono essere ripristinabili pubblicamente	[EC2.1] Le istantanee di Amazon EBS non devono essere configurate per essere ripristinabili pubblicamente
PCI DSS v3.2.1	PCI.EC2.2 Il gruppo di sicurezza predefinito VPC dovrebbe vietare il traffico in entrata e in uscita	[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
PCI DSS v3.2.1	PCI.EC2.4 Gli EIP EC2 non utilizzati devono essere rimossi	[EC2.12] Gli EIP Amazon EC2 non utilizzati devono essere rimossi
PCI DSS v3.2.1	PCI.EC2.5 I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alla porta 22	[EC2.13] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 22
PCI DSS v3.2.1	PCI.EC2.6 La registrazione del flusso VPC deve essere abilitata in tutti i VPC	[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC
PCI DSS v3.2.1	PCI.ELBv2.1 Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS	[ELB.1] Application Load Balancer deve essere configurato per reindiriz zare tutte le richieste HTTP a HTTPS
PCI DSS v3.2.1	PCI.ES.1 I domini Elasticsearch devono trovarsi in un VPC	[ES.2] I domini Elasticsearch non devono essere accessibili al pubblico
PCI DSS v3.2.1	PCI.ES.2 I domini Elasticsearch devono avere la crittografia a riposo abilitata	[ES.1] I domini Elasticsearch devono avere la crittografia a riposo abilitata
PCI DSS v3.2.1	PCI.GuardDuty.1 GuardDuty dovrebbe essere abilitato	[GuardDuty.1] GuardDuty dovrebbe essere abilitato
PCI DSS v3.2.1	PCI.IAM.1 La chiave di accesso utente root IAM non dovrebbe esistere	[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
PCI DSS v3.2.1	PCI.IAM.2 Gli utenti IAM non dovrebbero avere policy IAM allegate	[IAM.2] Gli utenti IAM non devono avere policy IAM allegate
PCI DSS v3.2.1	PCI.IAM.3 Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi	[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
PCI DSS v3.2.1	PCI.IAM.4 La MFA hardware deve essere abilitata per l'utente root	[IAM.6] La MFA hardware deve essere abilitata per l'utente root
PCI DSS v3.2.1	PCI.IAM.5 La MFA virtuale deve essere abilitata per l'utente root	[IAM.9] L'MFA deve essere abilitata per l'utente root
PCI DSS v3.2.1	PCI.IAM.6 L'MFA deve essere abilitata per tutti gli utenti IAM	[IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
PCI DSS v3.2.1	PCI.IAM.7 Le credenziali utente IAM devono essere disabilitate se non utilizzate entro un numero predefinito di giorni	[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
PCI DSS v3.2.1	PCI.IAM.8 Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide	[IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
PCI DSS v3.2.1	PCI.KMS.1 La rotazione della chiave principale del cliente (CMK) deve essere abilitata	[KMS.4] AWS KMS la rotazione dei tasti dovrebbe essere abilitata
PCI DSS v3.2.1	PCI.Lambda.1 Le funzioni Lambda dovrebbero vietare l'accesso pubblico	[Lambda.1] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico
PCI DSS v3.2.1	PCI.Lambda.2 Le funzioni Lambda devono trovarsi in un VPC	[Lambda.3] Le funzioni Lambda devono trovarsi in un VPC
PCI DSS v3.2.1	PCI.Opensearch.1 OpenSearch i domini devono essere in un VPC	[Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
PCI DSS v3.2.1	PCI.Opensearch.2 Le istantanee EBS non dovrebbero essere ripristin abili pubblicamente	[Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
PCI DSS v3.2.1	PCI.RDS.1 Le istantanee RDS devono essere private	[RDS.1] L'istantanea RDS deve essere privata
PCI DSS v3.2.1	PCI.RDS.2 Le istanze DB RDS devono vietare l'accesso pubblico	[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible
PCI DSS v3.2.1	PCI.Redshift.1 I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico	[Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico
PCI DSS v3.2.1	PCI.S3.1 I bucket S3 dovrebbero vietare l'accesso pubblico in scrittura	[S3.3] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura
PCI DSS v3.2.1	PCI.S3.2 I bucket S3 dovrebbero vietare l'accesso pubblico in lettura	[S3.2] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura
PCI DSS v3.2.1	PCI.S3.3 I bucket S3 devono avere la replica tra regioni abilitata	[S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni
PCI DSS v3.2.1	PCI.S3.5 I bucket S3 dovrebbero richiedere l'utilizzo di Secure Socket Layer	[S3.5] I bucket S3 per uso generico dovrebbero richiedere richieste di utilizzo di TLS
PCI DSS v3.2.1	PCI.S3.6 L'impostazione S3 Block Public Access deve essere abilitata	[S3.1] I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate
PCI DSS v3.2.1	PCI.SageMaker.1 Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet	[SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
PCI DSS v3.2.1	PCI.SSM.1 Le istanze EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch.	[SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch
PCI DSS v3.2.1	PCI.SSM.2 Le istanze EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT	[SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT
PCI DSS v3.2.1	PCI.SSM.3 Le istanze EC2 devono essere gestite da AWS Systems Manager	[SSM.1] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager

Aggiornamento dei flussi di lavoro per il consolidamento

Se i flussi di lavoro non si basano sul formato specifico di alcun campo nei risultati di controllo, non è richiesta alcuna azione.

Se i flussi di lavoro si basano sul formato specifico di uno o più campi nei risultati del controllo, come indicato nelle tabelle precedenti, è necessario aggiornare i flussi di lavoro. Ad esempio, se hai creato una EventBridge regola Amazon che ha attivato un'azione per un ID di controllo specifico, ad esempio richiamare una AWS Lambda funzione se l'ID di controllo è uguale a CIS 2.7, aggiorna la regola da CloudTrail.2 utilizzare, che è il valore del campo per `Compliance.SecurityControlId` quel controllo.

Se hai creato approfondimenti personalizzati che utilizzano uno dei campi o dei valori modificati, aggiorna tali approfondimenti per utilizzare i nuovi campi o valori.

Attributi ASFF di primo livello obbligatori

I seguenti attributi di primo livello nel AWS Security Finding Format (ASFF) sono necessari per tutti i risultati in Security Hub CSPM. Per ulteriori informazioni su questi attributi, vedere il riferimento AwsSecurityFindingall'API AWS Security Hub.

AwsAccountId

L' Account AWS ID a cui si riferisce il risultato.

Esempio

```
"AwsAccountId": "111111111111"
```

CreatedAt

Indica quando è stato creato il potenziale problema o evento di sicurezza rilevato da un risultato.

Esempio

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

Description

La descrizione di una ricerca. Questo campo può essere testo boilerplate non specifico o dettagli che sono specifici dell'istanza del risultato.

Per i risultati di controllo generati da Security Hub CSPM, questo campo fornisce una descrizione del controllo.

Questo campo non fa riferimento a uno standard se si attivano i risultati del controllo consolidato.

Esempio

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

L'identificatore per il componente specifico della soluzione (un'unità di logica discreta) che ha generato un risultato.

Per i risultati di controllo generati da Security Hub CSPM, questo campo non fa riferimento a uno standard se attivi i risultati del controllo consolidato.

Esempio

```
"GeneratorId": "security-control/Config.1"
```

Id

L'identificatore specifico del prodotto per un risultato. Per i risultati di controllo generati da Security Hub CSPM, questo campo fornisce l'Amazon Resource Name (ARN) del risultato.

Questo campo non fa riferimento a uno standard se attivi i risultati del controllo consolidato.

Esempio

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

L'Amazon Resource Name (ARN) generato da Security Hub CSPM che identifica in modo univoco un prodotto di ricerca di terze parti dopo la registrazione del prodotto presso Security Hub CSPM.

Il formato di questo campo è `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*.

- Servizi AWS Affinché siano integrati con Security Hub CSPM, `company-id` devono essere "`aws`«e `product-id` devono essere il nome del servizio AWS pubblico. Poiché AWS i prodotti e i servizi non sono associati a un account, la `account-id` sezione dell'ARN è vuota. Servizi AWS che non sono ancora integrati con Security Hub CSPM sono considerati prodotti di terze parti.
- Per prodotti pubblici, `company-id` e `product-id` devono essere i valori ID specificati al momento della registrazione.
- Per prodotti privati, `company-id` deve essere l'ID account. `product-id` deve essere la parola riservata "default" o l'ID specificato al momento della registrazione.

Esempio

```
// 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"
```

Resources

L'`Resources`array di oggetti fornisce una serie di tipi di dati relativi alle risorse che descrivono le AWS risorse a cui si riferisce il risultato. Per i dettagli sui campi che un `Resources` oggetto può contenere, inclusi i campi obbligatori, vedere il riferimento Resourceall'API AWS Security Hub. Per esempi di `Resources` oggetti specifici Servizi AWS, vedereResources Oggetto ASFF.

Esempio

```
"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

La versione dello schema per cui un risultato è formattato. Il valore di questo campo deve essere una delle versioni pubblicate ufficialmente identificate da AWS. Nella versione corrente, la versione dello schema AWS Security Finding Format è`2018-10-08`.

Esempio

```
"SchemaVersion": "2018-10-08"
```

Gravità

Definisce l'importanza di un risultato. Per i dettagli su questo oggetto, `Severity`consulta l'AWS Security Hub API Reference.

`Severity`è sia un oggetto di primo livello in una ricerca che annidato sotto l'`FindingProviderFields`oggetto.

Il valore dell'`Severity`oggetto di primo livello per un risultato deve essere aggiornato solo utilizzando l'API. `BatchUpdateFindings`

Per fornire informazioni sulla gravità, i provider di ricerca devono aggiornare l'`Severity`oggetto sotto `FindingProviderFields` quando effettuano una richiesta `BatchImportFindings`API.
Se una `BatchImportFindings` richiesta per un nuovo risultato fornisce solo `Label` o fornisce solo`Normalized`, Security Hub CSPM compila automaticamente il valore dell'altro campo. I `Original` campi `Product` e possono anche essere compilati.

Se l'`Finding.Severity`oggetto di primo livello è presente ma non lo `Finding.FindingProviderFields` è, Security Hub CSPM crea l'`FindingProviderFields.Severity`oggetto e copia l'intero `Finding.Severity object` in esso. Ciò garantisce che i dettagli originali forniti dal provider vengano mantenuti all'interno della `FindingProviderFields.Severity` struttura, anche se l'oggetto di primo livello viene sovrascritto. `Severity`

La gravità del risultato non considera la criticità degli asset coinvolti o della risorsa sottostante. La criticità è definita come il livello di importanza delle risorse associate al risultato. Ad esempio, una risorsa associata a un'applicazione mission critical ha una criticità maggiore rispetto a quella associata ai test non di produzione. Per acquisire informazioni sulla criticità delle risorse, utilizza il campo `Criticality`.

Si consiglia di utilizzare le seguenti indicazioni per tradurre i punteggi di gravità nativi dei risultati nel valore dell'ASFF. `Severity.Label`

- `INFORMATIONAL`— Questa categoria può includere un risultato relativo all'identificazione `PASSED` di `WARNING` dati sensibili o di `NOT AVAILABLE` controllo.
- `LOW`— Risultati che potrebbero portare a future compromessi. Ad esempio, questa categoria può includere vulnerabilità, punti deboli di configurazione e password esposte.
- `MEDIUM`— Risultati che indicano un compromesso attivo, ma nessuna indicazione che un avversario abbia raggiunto i propri obiettivi. Ad esempio, questa categoria può includere attività legate a malware, attività di hacking e rilevamento di comportamenti insoliti.
- `HIGH`oppure `CRITICAL` — Risultati che indicano che un avversario ha raggiunto i propri obiettivi, come la perdita o la compromissione attiva dei dati o l'interruzione del servizio.

Esempio

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

Titolo

Il titolo di un risultato. Questo campo può contenere testo boilerplate non specifico o dettagli specifici per l'istanza del risultato.

Per i risultati del controllo, questo campo fornisce il titolo del controllo. Questo campo non fa riferimento a uno standard se si attivano i risultati del controllo consolidato.

Esempio

```
"Title": "AWS Config should be enabled"
```

Tipi

Uno o più tipi di risultati nel formato *namespace*/*category*/*classifier* che classificano un risultato. Questo campo non fa riferimento a uno standard se attivi i risultati del controllo consolidato.

`Types`deve essere aggiornato solo utilizzando l'`BatchUpdateFindings`API.

La ricerca di fornitori che desiderano fornire un valore per `Types` deve utilizzare l'`Types`attributo sotto `FindingProviderFields`.

Nell'elenco seguente, i punti elenco di primo livello sono namespace, i punti elenco di secondo livello sono categorie e i punti elenco di terzo livello sono classificatori. Consigliamo che i provider di ricerca utilizzino namespace definiti per facilitare l'ordinamento e il raggruppamento dei risultati. È possibile utilizzare anche le categorie e i classificatori definiti, ma non sono obbligatori. Solo lo spazio dei nomi Software and Configuration Checks dispone di classificatori definiti.

È possibile definire un percorso parziale per /classifier. namespace/category Ad esempio, i seguenti tipi di ricerca sono tutti validi:

- TTPs
- TTPs/Defense Evasione
- TTPs/Defense Evasion/CloudTrailStopped

Le categorie di tattiche, tecniche e procedure (TTP) nell'elenco seguente si allineano al MITRE ATT&CK MatrixTM. Lo spazio dei nomi Unusual Behaviors riflette comportamenti insoliti generali, come anomalie statistiche generali, e non è allineato con un TTP specifico. Tuttavia, è possibile classificare un risultato con entrambi i tipi di risultato Unusual Behaviors e TTPs.

Elenco di namespace, categorie e classificatori:

- Software and Configuration Checks
  - Vulnerabilità
    - CVE

- AWS Migliori pratiche di sicurezza
  - Network Reachability
  - Runtime Behavior Analysis
- Industry and Regulatory Standards
  - AWS Migliori pratiche di sicurezza di base
  - CIS Host Hardening Benchmarks
  - Benchmark CIS Foundations AWS
  - PCI-DSS
  - Controlli Cloud Security Alliance
  - Controlli ISO 90001
  - Controlli ISO 27001
  - Controlli ISO 27017
  - Controlli ISO 27018
  - SOC 1
  - SOC 2
  - Controlli HIPAA (USA)
  - Controlli NIST 800-53 (USA)
  - Controlli NIST CSF (USA)
  - Controlli IRAP (Australia)
  - K-ISMS Controls (Corea)
  - Controlli MTCS (Singapore)
  - Controlli FISC (Giappone)
  - Controlli My Number Act (Giappone)
  - Controlli ENS (Spagna)
  - Controlli Cyber Essentials Plus (Regno Unito)
  - G-Cloud Controlli (Regno Unito)
  - Controlli C5 (Germania)
  - IT-Grundschutz Controls (Germania)
  - Controlli GDPR (Europa)

  - Controlli TISAX (Europa)

    - Gestione delle patch
- TTPs
    - Accesso iniziale
    - Esecuzione
    - Persistenza
    - Escalation dei privilegi
    - Defense Evasion
    - Accessi a credenziali
    - Individuazione
    - Movimento laterale
    - Raccolta
    - Comando e controllo
- Effetti
    - Esposizione di dati
    - Esfiltrazione di dati
    - Distruzione di dati
    - Denial of Service
    - Consumo di risorse
- Comportamenti insoliti
    - Applicazione
    - Flusso di rete
    - IP address (Indirizzo IP)
    - Utente
    - VM
    - Contenitore
    - Serverless
    - Processo
    - Database
    - Dati
- Identificazioni dati sensibili

- Informazioni che consentono l'identificazione personale degli utenti
- Password
- Note legali
- Servizi finanziari
- Sicurezza
- Business

Esempio

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
]
```

UpdatedAt

Indica quando il fornitore di ricerca ha aggiornato l'ultima volta il record dei risultati.

Questo timestamp indica l'ora in cui il record di ricerca è stato aggiornato l'ultima volta o l'ultimo aggiornamento. Di conseguenza, può differire dal `LastObservedAt` timestamp, che indica quando l'evento o la vulnerabilità sono stati osservati l'ultima volta o l'ultima volta.

Quando si aggiorna il record di risultato, è necessario aggiornare il timestamp al timestamp corrente. Al momento della creazione di un record di ricerca, i timestamp `CreatedAt` e i `UpdatedAt` timestamp devono essere gli stessi. Dopo un aggiornamento del record di ricerca, il valore di questo campo deve essere più recente di tutti i valori precedenti in esso contenuti.

Nota che `UpdatedAt` non può essere aggiornato utilizzando l'`BatchUpdateFindings`operazione. È possibile aggiornarlo solo utilizzando l'`BatchImportFindings`operazione.

Esempio

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Attributi ASFF di primo livello opzionali

I seguenti attributi di primo livello nel AWS Security Finding Format (ASFF) sono opzionali per i risultati in Security Hub CSPM. Per ulteriori informazioni su questi attributi, vedere il riferimento AwsSecurityFindingall'API AWS Security Hub.

Azione

L'`Action`oggetto fornisce dettagli su un'azione che influisce o è stata intrapresa su una risorsa.

Esempio

```
"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

Il Account AWS nome a cui si applica il risultato.

Esempio

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

Il nome dell'azienda del prodotto che ha generato il risultato. Per i risultati basati sul controllo, la società è. AWS

Security Hub CSPM compila automaticamente questo attributo per ogni risultato. Non è possibile aggiornarlo utilizzando o. `BatchImportFindings` `BatchUpdateFindings` L'eccezione è quando si utilizza un'integrazione personalizzata. Consulta the section called "Integrazioni di prodotti personalizzate".

Quando si utilizza la console CSPM di Security Hub per filtrare i risultati in base al nome dell'azienda, si utilizza questo attributo. Quando si utilizza l'API CSPM Security Hub per filtrare i risultati in base al nome dell'azienda, si utilizza l'`aws/securityhub/CompanyName`attributo sotto. `ProductFields` Security Hub CSPM non sincronizza questi due attributi.

Esempio

```
"CompanyName": "AWS"
```

Conformità

L'`Compliance`oggetto fornisce in genere dettagli su un risultato di controllo, come gli standard applicabili e lo stato del controllo.

Esempio

```
"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."
        }
    ]
}
```

Confidence

La probabilità che un risultato identifichi accuratamente il comportamento o il problema che intendeva identificare.

`Confidence`deve essere aggiornato solo utilizzando. `BatchUpdateFindings`

La ricerca di fornitori che desiderano fornire un valore per `Confidence` dovrebbe utilizzare l'`Confidence`attributo sotto`FindingProviderFields`. Consulta the section called "Aggiornamento dei risultati con FindingProviderFields".

`Confidence`viene assegnato un punteggio da 0 a 100 utilizzando una scala di rapporti. 0 significa confidenza dello 0% e 100 indica una confidenza del 100 percento. Ad esempio, un rilevamento di un'esfiltrazione di dati basato su una deviazione statistica del traffico di rete ha una bassa affidabilità perché non è stata verificata un'effettiva esfiltrazione.

Esempio

```
"Confidence": 42
```

Criticità

Il livello di importanza assegnato alle risorse associate a un risultato.

`Criticality`deve essere aggiornato solo chiamando l'operazione `BatchUpdateFindings`API. Non aggiornare questo oggetto con `BatchImportFindings`.

La ricerca di fornitori che desiderano fornire un valore per `Criticality` deve utilizzare l'`Criticality`attributo sotto`FindingProviderFields`. Consulta the section called "Aggiornamento dei risultati con FindingProviderFields".

`Criticality`viene assegnato un punteggio da 0 a 100, utilizzando una scala di rapporti che supporta solo numeri interi completi. Un punteggio 0 indica che le risorse sottostanti non presentano criticità, mentre un punteggio 100 è riservato per la maggior parte delle risorse critiche.

Per ogni risorsa, al momento dell'assegnazione, tenete presente quanto segue: `Criticality`

- La risorsa interessata contiene dati sensibili (ad esempio, un bucket S3 con PII)?
- La risorsa interessata consente a un avversario di approfondire il proprio accesso o di estendere le proprie capacità per svolgere attività dannose aggiuntive (ad esempio, un account sysadmin compromesso)?
- La risorsa è un asset critico per l'azienda (ad esempio, un sistema aziendale chiave che se compromesso potrebbe avere un impatto notevole sui profitti)?

Puoi utilizzare le linee guida seguenti:

- Una risorsa che alimenta sistemi mission-critical o che contiene dati altamente sensibili può essere valutata nell'intervallo 75-100.
- Una risorsa che alimenta sistemi importanti (ma non critici) o che contiene dati moderatamente importanti può essere valutata nell'intervallo 25-74.
- Una risorsa che alimenta sistemi non importanti o che contiene dati non sensibili dovrebbe avere un punteggio compreso tra 0 e 24.

Esempio

```
"Criticality": 99
```

Rilevamento

L'`Detection`oggetto fornisce dettagli sulla sequenza di attacco rilevata da Amazon GuardDuty Extended Threat Detection. GuardDuty genera una sequenza di attacco che rileva quando più eventi si allineano a un'attività potenzialmente sospetta. Per ricevere i risultati della sequenza di GuardDuty attacco in AWS Security Hub CSPM, devi averlo GuardDuty abilitato nel tuo account. Per ulteriori informazioni, consulta Amazon GuardDuty Extended Threat Detection nella Amazon GuardDuty User Guide.

Esempio

```
"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`include i seguenti attributi:

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

I campi precedenti sono annidati sotto l'`FindingProviderFields`oggetto, ma hanno analoghi con lo stesso nome dei campi ASFF di primo livello. Quando un nuovo risultato viene inviato a Security Hub CSPM da un provider di ricerca, Security Hub CSPM popola automaticamente l'`FindingProviderFields`oggetto se è vuoto in base ai campi di primo livello corrispondenti.

Finding provider può eseguire l'aggiornamento `FindingProviderFields` utilizzando il `BatchImportFindings`funzionamento dell'API CSPM Security Hub. I provider di Finding non possono aggiornare questo oggetto con. `BatchUpdateFindings`

Per i dettagli su come Security Hub CSPM gestisce gli aggiornamenti da `FindingProviderFields` e `BatchImportFindings` verso gli attributi di primo livello corrispondenti, vedere. the section called "Aggiornamento dei risultati con FindingProviderFields"

I clienti possono aggiornare i campi di primo livello utilizzando l'operazione. `BatchUpdateFindings` I clienti non possono effettuare l'aggiornamento`FindingProviderFields`.

Esempio

```
"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

Indica quando il potenziale problema o evento di sicurezza rilevato da un risultato è stato osservato per la prima volta.

Questo timestamp specifica quando l'evento o la vulnerabilità sono stati osservati per la prima volta. Di conseguenza, può differire dal `CreatedAt` timestamp, che indica quando è stato creato questo record di risultati.

Per quanto riguarda i risultati di controllo generati e aggiornati da Security Hub CSPM, questo timestamp può anche indicare quando lo stato di conformità di una risorsa è cambiato più di recente. Per altri tipi di risultati, questo timestamp deve essere immutabile tra un aggiornamento e l'altro del record dei risultati, ma può essere aggiornato se viene determinato un timestamp più preciso.

Esempio

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Indica quando il potenziale problema o evento di sicurezza rilevato da un risultato è stato osservato più di recente dal prodotto Security Finds.

Questo timestamp specifica quando l'evento o la vulnerabilità sono stati osservati l'ultima volta o l'ultima volta. Di conseguenza, può differire dal `UpdatedAt` timestamp, che indica quando questo record di risultati è stato aggiornato l'ultima volta o l'ultimo aggiornamento.

È possibile fornire questo timestamp, ma non è richiesto alla prima osservazione. Se compili questo campo alla prima osservazione, il timestamp dovrebbe essere lo stesso del timestamp. `FirstObservedAt` Aggiornare questo campo per riflettere l'ultimo timestamp o il timestamp osservato più di recente ogni volta che un risultato viene osservato.

Esempio

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

L'oggetto `Malware` fornisce un elenco di malware relativo a una ricerca.

Esempio

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

Rete (ritirata)

L'`Network`oggetto fornisce informazioni relative alla rete su un risultato.

Questo oggetto è stato ritirato. Per fornire questi dati, è possibile mappare i dati a una risorsa in `Resources` o utilizzare l'`Action`oggetto.

Esempio

```
"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

L'`NetworkPath`oggetto fornisce informazioni su un percorso di rete correlato a un risultato. Ogni voce in `NetworkPath` rappresenta un componente del percorso.

Esempio

```
"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" ]
            }
        }
```

```
    }
]
```

Nota

L'`Note`oggetto specifica una nota definita dall'utente che è possibile aggiungere a un risultato.

Un provider di risultati può fornire una nota iniziale per una ricerca, ma non può aggiungere note successivamente. È possibile aggiornare una nota solo utilizzando. `BatchUpdateFindings`

Esempio

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

L'`PatchSummary`oggetto fornisce un riepilogo dello stato di conformità della patch per un'istanza rispetto a uno standard di conformità selezionato.

Esempio

```
"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"
}
```

Processo

L'`Process`oggetto fornisce dettagli relativi al processo relativi a un risultato.

Esempio:

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Indica quando Security Hub CSPM ha ricevuto un risultato e ha iniziato a elaborarlo.

Ciò differisce da `CreatedAt` e`UpdatedAt`, che sono timestamp obbligatori relativi all'interazione del fornitore dei risultati con il problema e la scoperta di sicurezza. Il `ProcessedAt` timestamp indica quando Security Hub CSPM inizia a elaborare un risultato. Una volta completata l'elaborazione, viene visualizzato un risultato nell'account di un utente.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Un tipo di dati in cui i prodotti per i risultati della sicurezza possono includere dettagli aggiuntivi specifici della soluzione che non fanno parte del AWS Security Finding Format definito.

Per i risultati generati dai controlli CSPM di Security Hub, `ProductFields` include informazioni sul controllo. Consulta the section called "Generazione e aggiornamento dei risultati di controllo".

Questo campo non deve contenere dati ridondanti e non deve contenere dati in conflitto con i campi del AWS Security Finding Format.

Il prefisso `aws/` "" rappresenta uno spazio dei nomi riservato solo a AWS prodotti e servizi e non deve essere associato ai risultati di integrazioni di terze parti.

Anche se non richiesto, i nomi di campo dei prodotti devono avere il formato `company-id/product-id/field-name`, in cui `company-id` e `product-id` corrispondono a quelli forniti nella `ProductArn` del risultato.

I campi a cui si fa riferimento `Archival` vengono utilizzati quando Security Hub CSPM archivia un risultato esistente. Ad esempio, Security Hub CSPM archivia i risultati esistenti quando si disabilita un controllo o uno standard e quando si attivano o disattivano i risultati del controllo consolidato.

Questo campo può includere anche informazioni sullo standard che include il controllo che ha prodotto il risultato.

Esempio

```
"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

Fornisce il nome del prodotto che ha generato il risultato. Per i risultati basati sul controllo, il nome del prodotto è Security Hub CSPM.

Security Hub CSPM compila automaticamente questo attributo per ogni risultato. Non è possibile aggiornarlo utilizzando o. `BatchImportFindings` `BatchUpdateFindings` L'eccezione è quando si utilizza un'integrazione personalizzata. Consulta the section called "Integrazioni di prodotti personalizzate".

Quando si utilizza la console CSPM di Security Hub per filtrare i risultati in base al nome del prodotto, si utilizza questo attributo.

Quando si utilizza l'API CSPM Security Hub per filtrare i risultati in base al nome del prodotto, si utilizza l'`aws/securityhub/ProductName`attributo sotto. `ProductFields`

Security Hub CSPM non sincronizza questi due attributi.

RecordState

Fornisce lo stato di registrazione di un risultato.

Per impostazione predefinita, i risultati inizialmente generati da un servizio sono considerati `ACTIVE`.

Lo stato `ARCHIVED` indica che un risultato deve essere nascosto dalla vista. I risultati archiviati non vengono eliminati immediatamente. Puoi cercarli, esaminarli e riferirli. Security Hub CSPM archivia automaticamente i risultati basati sul controllo se la risorsa associata viene eliminata, la risorsa non esiste o il controllo è disabilitato.

`RecordState`è destinato alla ricerca di fornitori e può essere aggiornato solo utilizzando l'operazione. `BatchImportFindings` Non è possibile aggiornarlo utilizzando l'`BatchUpdateFindings`operazione.

Per tenere traccia dello stato della tua indagine su un risultato, usa `Workflow`invece di`RecordState`.

Se lo stato del record cambia da `ARCHIVED` a `ACTIVE` e lo stato del flusso di lavoro del risultato è `NOTIFIED` o`RESOLVED`, Security Hub CSPM modifica automaticamente lo stato del flusso di lavoro in. `NEW`

Esempio

```
"RecordState": "ACTIVE"
```

Region

Speciifica il risultato Regione AWS da cui è stato generato il risultato.

Security Hub CSPM compila automaticamente questo attributo per ogni risultato. Non è possibile aggiornarlo utilizzando o. `BatchImportFindings``BatchUpdateFindings`

Esempio

```
"Region": "us-west-2"
```

RelatedFindings

Fornisce un elenco di risultati correlati al risultato corrente.

`RelatedFindings`deve essere aggiornato solo con l'operazione `BatchUpdateFindings`API. Non dovresti aggiornare questo oggetto con `BatchImportFindings`.

Per `BatchImportFindings`le richieste, i provider di ricerca devono utilizzare l'`RelatedFindings`oggetto sotto `FindingProviderFields`.

Per visualizzare le descrizioni degli `RelatedFindings` attributi, `RelatedFinding`consulta l'AWS Security Hub API Reference.

Esempio

```
"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

Esempio

```
"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"
                    }
                ]
            }
        ]
    }
}
```

Correzione

L'oggetto `Remediation` fornisce informazioni sulle procedure di correzione consigliate per risolvere la ricerca.

Esempio

```
"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"
    }
}
```

Project N.E.M.O.

Speciifica se il risultato è un risultato di esempio.

```
"Sample": true
```

SourceUrl

L'`SourceUrl`oggetto fornisce un URL che rimanda a una pagina relativa alla scoperta corrente del prodotto oggetto della ricerca.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

L'`ThreatIntelIndicator`oggetto fornisce dettagli di intelligence sulle minacce correlati a una scoperta.

Esempio

```
"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",
  }
]
```

Minacce

L'Threatsoggetto fornisce dettagli sulla minaccia rilevata da un risultato.

Esempio

```
"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

Fornisce un elenco di coppie di stringhe nome-valore associate al risultato. Si tratta di campi personalizzati, definiti dall'utente che vengono aggiunti a un risultato. Questi campi possono essere generati automaticamente tramite una configurazione specifica.

I fornitori di servizi di ricerca non devono utilizzare questo campo per i dati generati dal prodotto. Invece, i provider di ricerca possono utilizzare il `ProductFields` campo per i dati che non sono mappati a nessun campo standard del AWS Security Finding Format.

Questi campi possono essere aggiornati solo utilizzando `BatchUpdateFindings`.

Esempio

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

Fornisce la veridicità di un risultato. I prodotti Findings possono fornire un valore di `UNKNOWN` per questo campo. Un prodotto dei risultati dovrebbe fornire un valore per questo campo se esiste un analogo significativo nel sistema del prodotto dei risultati. Questo campo viene in genere compilato in base alla determinazione o all'azione dell'utente dopo l'analisi di un risultato.

Un provider di risultati può fornire un valore iniziale per questo attributo, ma non può aggiornarlo successivamente. È possibile aggiornare questo attributo solo utilizzando. `BatchUpdateFindings`

```
"VerificationState": "Confirmed"
```

Vulnerabilità

L'Vulnerabilitiesoggetto fornisce un elenco di vulnerabilità associate a un risultato.

Esempio


```
"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"
            }
        ]
    }
]
```

Flusso di lavoro

L' oggetto `Workflow` fornisce informazioni sullo stato dell'indagine su un risultato.

Questo campo è destinato ai clienti da utilizzare con strumenti di correzione, orchestrazione e ticketing. Non è destinato per provider di risultati.

Puoi aggiornare il campo solo con. `Workflow` `BatchUpdateFindings` I clienti possono anche aggiornarlo dalla console. Consulta the section called "Impostazione dello stato dei risultati del flusso di lavoro".

Esempio

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState (Ritirato)

Questo oggetto è stato ritirato ed è stato sostituito dal `Status` campo dell'`Workflow`oggetto.

Questo campo fornisce lo stato del flusso di lavoro di un risultato. I prodotti dei risultati sono in grado di fornire il valore di `NEW` per questo campo. Un prodotto dei risultati è in grado di fornire un valore per questo campo se esiste un analogo significativo nel sistema del prodotto dei risultati.

Esempio

```
"WorkflowState": "NEW"
```

Resources Oggetto ASFF

Nel AWS Security Finding Format (ASFF), l'`Resources`oggetto fornisce informazioni sulle risorse coinvolte in una ricerca. Contiene una matrice di un massimo di 32 oggetti risorsa. Per determinare come vengono formattati i nomi delle risorse, vedereAWS Formato ASFF (Security Finding Format). Per esempi di ogni oggetto risorsa, selezionate una risorsa dall'elenco seguente.

Argomenti

- Attributi delle risorse nell'ASFF
- AwsAmazonMQ risorse in ASFF
- AwsApiGateway risorse in ASFF
- AwsAppSync risorse in ASFF
- AwsAthena risorse in ASFF
- AwsAutoScaling risorse in ASFF
- AwsBackup risorse in ASFF
- AwsCertificateManager risorse in ASFF
- AwsCloudFormation risorse in ASFF
- AwsCloudFront risorse in ASFF
- AwsCloudTrail risorse in ASFF
- AwsCloudWatch risorse in ASFF
- AwsCodeBuild risorse in ASFF
- AwsDms risorse in ASFF
- AwsDynamoDB risorse in ASFF
- AwsEc2 risorse in ASFF
- AwsEcr risorse in ASFF

- AwsEcs risorse in ASFF
- AwsEfs risorse in ASFF
- AwsEks risorse in ASFF
- AwsElasticBeanstalk risorse in ASFF
- AwsElasticSearch risorse in ASFF
- AwsElb risorse in ASFF
- AwsEventBridge risorse in ASFF
- AwsGuardDuty risorse in ASFF
- AwsIam risorse in ASFF
- AwsKinesis risorse in ASFF
- AwsKms risorse in ASFF
- AwsLambda
- AwsMsk risorse in ASFF
- AwsNetworkFirewall risorse in ASFF
- AwsOpenSearchService risorse in ASFF
- AwsRds risorse in ASFF
- AwsRedshift risorse in ASFF
- AwsRoute53 risorse in ASFF
- AWS 3 risorse in ASFF
- AwsSageMaker risorse in ASFF
- AwsSecretsManager risorse in ASFF
- AwsSns risorse in ASFF
- AwsSqs risorse in ASFF
- AwsSsm risorse in ASFF
- AwsStepFunctions risorse in ASFF
- AwsWaf risorse in ASFF
- AwsXray risorse in ASFF
- CodeRepository oggetto in ASFF
- Contenitore oggetto in ASFF
- Altro oggetto in ASFF

Attributi delle risorse nell'ASFF

Di seguito sono riportate le descrizioni e gli esempi dell'`Resources`oggetto nel AWS Security Finding Format (ASFF). Per ulteriori informazioni sui campi, consulta Resources.

ApplicationArn

Identifica l'Amazon Resource Name (ARN) dell'applicazione coinvolta nella scoperta.

Esempio

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

Identifica il nome dell'applicazione coinvolta nella scoperta.

Esempio

```
"ApplicationName": "SampleApp"
```

DataClassification

Il DataClassificationcampo fornisce informazioni sui dati sensibili rilevati sulla risorsa.

Esempio

```
"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
    }
  }
}
```

Informazioni

Il Detailscampo fornisce informazioni aggiuntive su una singola risorsa utilizzando gli oggetti appropriati. Ogni risorsa deve essere fornita in un oggetto risorsa separato nell'`Resources`oggetto.

Si noti che se la dimensione del risultato supera il massimo di 240 KB, l'`Details`oggetto viene rimosso dal risultato. Per i risultati del controllo che utilizzano AWS Config regole, è possibile visualizzare i dettagli delle risorse sulla AWS Config console.

Security Hub CSPM fornisce una serie di dettagli sulle risorse disponibili per i tipi di risorse supportati. Questi dettagli corrispondono ai valori dell'`Type`oggetto. Usa i tipi forniti quando possibile.

Ad esempio, se la risorsa è un bucket S3, imposta la risorsa `Type` su `AwsS3Bucket` e fornisci i dettagli della risorsa nell'`AwsS3Bucket`oggetto.

L'`Other`oggetto consente di fornire campi e valori personalizzati. L'`Other`oggetto viene utilizzato nei seguenti casi:

- Il tipo di risorsa (il valore della risorsa`Type`) non ha un oggetto di dettaglio corrispondente. Per fornire dettagli sulla risorsa, si utilizza l'`Other`oggetto.
- L'oggetto per il tipo di risorsa non include tutti i campi che si desidera compilare. In questo caso, utilizzate l'oggetto di dettaglio relativo al tipo di risorsa per compilare i campi disponibili. Utilizzate l'`Other`oggetto per compilare i campi che non si trovano nell'oggetto specifico del tipo.
- Il tipo di risorsa non è uno dei tipi forniti. In questo caso, `Resource.Type` impostate `Other` e utilizzate l'`Other`oggetto per compilare i dettagli.

Esempio

```
"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

L'identificatore per il tipo di risorsa specificato.

Per AWS le risorse identificate da Amazon Resource Names (ARN), questo è l'ARN.

Per AWS le risorse prive di ARN, questo è l'identificatore definito dal AWS servizio che ha creato la risorsa.

Per le non AWS risorse, si tratta di un identificatore univoco associato alla risorsa.

Esempio

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

Partizione

La partizione in cui si trova la risorsa. Una partizione è un gruppo di. Regioni AWS Ciascuno Account AWS è limitato a una partizione.

Sono supportate le seguenti partizioni:

- `aws` – Regioni AWS
- `aws-cn` - Regioni Cina
- `aws-us-gov` – AWS GovCloud (US) Region

Esempio

```
"Partition": "aws"
```

Region

Il codice del Regione AWS luogo in cui si trova questa risorsa. Per un elenco dei codici regionali, consulta Endpoint regionali.

Esempio

```
"Region": "us-west-2"
```

ResourceRole

Identifica il ruolo della risorsa nella scoperta. Una risorsa è l'obiettivo dell'attività di ricerca o l'attore che ha eseguito l'attività.

Esempio

```
"ResourceRole": "target"
```

Tag

Questo campo fornisce informazioni sulla chiave e sul valore dei tag per la risorsa coinvolta in una ricerca. È possibile etichettare le risorse supportate dal `GetResources` funzionamento dell'API AWS Resource Groups Tagging. Security Hub CSPM richiama questa operazione tramite il ruolo collegato al servizio e recupera i tag delle risorse se il `Resource.Id` campo AWS Security Finding Format (ASFF) è popolato con l'ARN della risorsa. AWS Gli ID di risorsa non validi vengono ignorati.

Puoi aggiungere tag di risorse ai risultati che Security Hub CSPM acquisisce, inclusi i risultati di prodotti integrati Servizi AWS e di terze parti.

L'aggiunta di tag consente di visualizzare i tag associati a una risorsa al momento dell'elaborazione del risultato. È possibile includere l'`Tags`attributo solo per le risorse a cui è associato un tag. Se a una risorsa non è associato un tag, non includere un attributo `Tags` nel risultato.

L'inclusione dei tag delle risorse nei risultati elimina la necessità di creare pipeline di arricchimento dei dati o di arricchire manualmente i metadati dei risultati di sicurezza. Puoi anche utilizzare i tag per cercare o filtrare risultati e approfondimenti e creare regole di automazione.

Per informazioni sulle restrizioni che si applicano ai tag, consulta Limiti e requisiti di denominazione dei tag.

In questo campo puoi fornire solo i tag che esistono su una AWS risorsa. Per fornire dati che non sono definiti nel AWS Security Finding Format, utilizza il sottocampo dei `Other` dettagli.

Esempio

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Tipo

Il tipo di risorsa per cui stai fornendo i dettagli.

Quando possibile, utilizza uno dei tipi di risorse forniti, ad esempio `AwsEc2Instance` o `AwsS3Bucket`.

Se il tipo di risorsa non corrisponde a nessuno dei tipi di risorsa forniti, imposta la risorsa `Type` su e utilizza il sottocampo dei `Other` dettagli per compilare i dettagli. `Other`

I valori supportati sono elencati in Risorse.

Esempio

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi del AWS Security Finding Format (ASFF) per le `AwsAmazonMQ` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsAmazonMQBroker

`AwsAmazonMQBroker`fornisce informazioni su un broker Amazon MQ, che è un ambiente di broker di messaggi in esecuzione su Amazon MQ.

L'esempio seguente mostra l'ASFF per l'`AwsAmazonMQBroker`oggetto. Per visualizzare le descrizioni degli `AwsAmazonMQBroker` attributi, consulta AwsAmazonMQBrokerl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsApiGateway` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsApiGatewayRestApi

L'`AwsApiGatewayRestApi`oggetto contiene informazioni su un'API REST nella versione 1 di Amazon API Gateway.

Di seguito è riportato un esempio di `AwsApiGatewayRestApi` ricerca nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayRestApi` attributi, consulta AwsApiGatewayRestApiDetailsl'AWS Security Hub API Reference.

Esempio

```
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

L'`AwsApiGatewayStage`oggetto fornisce informazioni su una fase di Amazon API Gateway versione 1.

Di seguito è riportato un esempio di `AwsApiGatewayStage` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayStage` attributi, consulta AwsApiGatewayStageDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsApiGatewayV2Api`oggetto contiene informazioni su un'API versione 2 in Amazon API Gateway.

Di seguito è riportato un esempio di `AwsApiGatewayV2Api` ricerca nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayV2Api` attributi, consulta AwsApiGatewayV2ApiDetailsl'AWS Security Hub API Reference.

Esempio

```
"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`contiene informazioni sulla versione 2 (fase) per Amazon API Gateway.

Di seguito è riportato un esempio di `AwsApiGatewayV2Stage` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayV2Stage` attributi, consulta AwsApiGatewayV2StageDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsAppSync` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsAppSyncGraphQLApi

`AwsAppSyncGraphQLApi`fornisce informazioni su un'API AWS AppSync GraphQL, che è un costrutto di primo livello per l'applicazione.

L'esempio seguente mostra l'ASFF per l'oggetto. `AwsAppSyncGraphQLApi` Per visualizzare le descrizioni degli `AwsAppSyncGraphQLApi` attributi, consulta AwsAppSyncGraphQLApil'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsAthena`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsAthenaWorkGroup

`AwsAthenaWorkGroup`fornisce informazioni su un gruppo di lavoro Amazon Athena. Un gruppo di lavoro ti aiuta a separare utenti, team, applicazioni o carichi di lavoro. Inoltre, consente di impostare limiti all'elaborazione dei dati e tenere traccia dei costi.

L'esempio seguente mostra l'ASFF per l'`AwsAthenaWorkGroup`oggetto. Per visualizzare le descrizioni degli `AwsAthenaWorkGroup` attributi, consulta AwsAthenaWorkGroupl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsAutoScaling`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsAutoScalingAutoScalingGroup

L'`AwsAutoScalingAutoScalingGroup`oggetto fornisce dettagli su un gruppo di ridimensionamento automatico.

Di seguito è riportato un esempio di `AwsAutoScalingAutoScalingGroup` ricerca nel AWS Security Finding Format (ASFF). Per visualizzare le

descrizioni degli `AwsAutoScalingAutoScalingGroup` attributi, consulta AwsAutoScalingAutoScalingGroupDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsAutoScalingLaunchConfiguration`oggetto fornisce dettagli sulla configurazione di avvio.

Di seguito è riportato un esempio di `AwsAutoScalingLaunchConfiguration` ricerca nel AWS Security Finding Format (ASFF).

Per visualizzare le descrizioni degli `AwsAutoScalingLaunchConfiguration` attributi, consulta AwsAutoScalingLaunchConfigurationDetailsl'AWS Security Hub API Reference.

Esempio

```
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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsBackup` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsBackupBackupPlan

L'`AwsBackupBackupPlan`oggetto fornisce informazioni su un piano AWS Backup di backup. Un piano di AWS Backup backup è un'espressione politica che definisce quando e come si desidera eseguire il backup AWS delle risorse.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsBackupBackupPlan`oggetto. Per visualizzare le descrizioni degli `AwsBackupBackupPlan` attributi, consulta AwsBackupBackupPlanl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsBackupBackupVault`oggetto fornisce informazioni su un archivio AWS Backup di backup. Un archivio AWS Backup di backup è un contenitore che archivia e organizza i backup.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsBackupBackupVault` Per visualizzare le descrizioni degli `AwsBackupBackupVault` attributi, consulta AwsBackupBackupVaultl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsBackupRecoveryPoint`oggetto fornisce informazioni su un AWS Backup backup, noto anche come punto di ripristino. Un punto di AWS Backup ripristino rappresenta il contenuto di una risorsa in un momento specifico.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsBackupRecoveryPoint`oggetto. Per visualizzare le descrizioni degli `AwsBackupBackupVault` attributi, consulta AwsBackupRecoveryPointl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsCertificateManager`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsCertificateManagerCertificate

L'`AwsCertificateManagerCertificate`oggetto fornisce dettagli su un certificato AWS Certificate Manager (ACM).

Di seguito è riportato un esempio di `AwsCertificateManagerCertificate` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsCertificateManagerCertificate` attributi, consulta AwsCertificateManagerCertificateDetailsl'AWS Security Hub API Reference.

Esempio


```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsCloudFormation` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsCloudFormationStack

L'`AwsCloudFormationStack`oggetto fornisce dettagli su uno AWS CloudFormation stack annidato come risorsa in un modello di primo livello.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsCloudFormationStack` Per visualizzare le descrizioni degli `AwsCloudFormationStack` attributi, consulta AwsCloudFormationStackDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsCloudFront` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsCloudFrontDistribution

L'`AwsCloudFrontDistribution`oggetto fornisce dettagli su una configurazione di CloudFront distribuzione Amazon.

Di seguito è riportato un esempio di `AwsCloudFrontDistribution` ricerca nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsCloudFrontDistribution` attributi, consulta AwsCloudFrontDistributionDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsCloudTrail` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsCloudTrailTrail

L'`AwsCloudTrailTrail`oggetto fornisce dettagli su un AWS CloudTrail percorso.

Di seguito è riportato un esempio di `AwsCloudTrailTrail` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsCloudTrailTrail` attributi, consulta AwsCloudTrailTrailDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsCloudWatch` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsCloudWatchAlarm

L'`AwsCloudWatchAlarm`oggetto fornisce dettagli sugli CloudWatch allarmi Amazon che controllano una metrica o eseguono un'azione quando un allarme cambia stato.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsCloudWatchAlarm` Per visualizzare le descrizioni degli `AwsCloudWatchAlarm` attributi, consulta AwsCloudWatchAlarmDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsCodeBuild` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsCodeBuildProject

L'oggetto `AwsCodeBuildProject` fornisce informazioni su un progetto AWS CodeBuild .

Di seguito è riportato un esempio di `AwsCodeBuildProject` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsCodeBuildProject` attributi, consulta AwsCodeBuildProjectDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsDms` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsDmsEndpoint

L'`AwsDmsEndpoint`oggetto fornisce informazioni su un endpoint AWS Database Migration Service (AWS DMS). Un endpoint fornisce informazioni sulla connessione, sul tipo di data store e sulla posizione del data store.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsDmsEndpoint`oggetto. Per visualizzare le descrizioni degli `AwsDmsEndpoint` attributi, consulta AwsDmsEndpointDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsDmsReplicationInstance`oggetto fornisce informazioni su un'istanza di replica AWS Database Migration Service (AWS DMS). DMS utilizza un'istanza di replica per connettersi al data store di origine, leggere i dati di origine e formattare i dati per l'utilizzo da parte del data store di destinazione.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsDmsReplicationInstance` Per visualizzare le descrizioni degli `AwsDmsReplicationInstance` attributi, consulta AwsDmsReplicationInstanceDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsDmsReplicationTask`oggetto fornisce informazioni su un'attività di replica AWS Database Migration Service (AWS DMS). Un'attività di replica sposta un set di dati dall'endpoint di origine all'endpoint di destinazione.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsDmsReplicationInstance` Per visualizzare le descrizioni degli `AwsDmsReplicationInstance` attributi, consulta AwsDmsReplicationInstancel'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsDynamoDB`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsDynamoDbTable

L'`AwsDynamoDbTable`oggetto fornisce dettagli su una tabella Amazon DynamoDB.

Di seguito è riportato un esempio di `AwsDynamoDbTable` ricerca nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsDynamoDbTable` attributi, consulta AwsDynamoDbTableDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsEc2`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsEc2ClientVpnEndpoint

L'`AwsEc2ClientVpnEndpoint`oggetto fornisce informazioni su un AWS Client VPN endpoint. Un endpoint Client VPN è la risorsa che crei e configuri per abilitare e gestire le sessioni VPN client. È il punto di chiusura per tutte le sessioni VPN client.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEc2ClientVpnEndpoint`oggetto. Per visualizzare le descrizioni degli `AwsEc2ClientVpnEndpoint` attributi, consulta AwsEc2ClientVpnEndpointDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2Eip`oggetto fornisce informazioni su un indirizzo IP elastico.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEc2Eip`oggetto. Per visualizzare le descrizioni degli `AwsEc2Eip` attributi, consulta AwsEc2EipDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2Instance`oggetto fornisce dettagli su un'istanza Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEc2Instance`oggetto. Per visualizzare le descrizioni degli `AwsEc2Instance` attributi, consulta AwsEc2InstanceDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2LaunchTemplate`oggetto contiene dettagli su un modello di lancio di Amazon Elastic Compute Cloud che specifica le informazioni di configurazione dell'istanza.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsEc2LaunchTemplate` Per visualizzare le descrizioni degli `AwsEc2LaunchTemplate` attributi, consulta AwsEc2LaunchTemplateDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2NetworkAcl`oggetto contiene dettagli su una lista di controllo degli accessi alla rete (ACL) di Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsEc2NetworkAcl` Per visualizzare le descrizioni degli `AwsEc2NetworkAcl` attributi, consulta AwsEc2NetworkAclDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2NetworkInterface`oggetto fornisce informazioni su un'interfaccia di rete Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEc2NetworkInterface`oggetto. Per visualizzare le descrizioni degli `AwsEc2NetworkInterface` attributi, consulta AwsEc2NetworkInterfaceDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2RouteTable`oggetto fornisce informazioni su una tabella di routing di Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEc2RouteTable`oggetto. Per visualizzare le descrizioni degli `AwsEc2RouteTable` attributi, consulta AwsEc2RouteTableDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2SecurityGroup`oggetto descrive un gruppo di sicurezza Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEc2SecurityGroup`oggetto. Per visualizzare le descrizioni degli `AwsEc2SecurityGroup` attributi, consulta AwsEc2SecurityGroupDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2Subnet`oggetto fornisce informazioni su una sottorete in Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsEc2Subnet` Per visualizzare le descrizioni degli `AwsEc2Subnet` attributi, consulta AwsEc2SubnetDetailsl'AWS Security Hub API Reference.

Esempio

```
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

L'`AwsEc2TransitGateway`oggetto fornisce dettagli su un gateway di transito Amazon EC2 che interconnette i cloud privati virtuali (VPC) e le reti locali.

Di seguito è riportato un esempio di `AwsEc2TransitGateway` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsEc2TransitGateway` attributi, consulta AwsEc2TransitGatewayDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2Volume`oggetto fornisce dettagli su un volume Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEc2Volume`oggetto. Per visualizzare le descrizioni degli `AwsEc2Volume` attributi, consulta AwsEc2VolumeDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2Vpc`oggetto fornisce dettagli su un VPC Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsEc2Vpc` Per visualizzare le descrizioni degli `AwsEc2Vpc` attributi, consulta AwsEc2VpcDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2VpcEndpointService`oggetto contiene dettagli sulla configurazione del servizio per un servizio endpoint VPC.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsEc2VpcEndpointService` Per visualizzare le descrizioni degli `AwsEc2VpcEndpointService` attributi, consulta AwsEc2VpcEndpointServiceDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEc2VpcPeeringConnection`oggetto fornisce dettagli sulla connessione di rete tra due VPC.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEc2VpcPeeringConnection`oggetto. Per visualizzare le descrizioni degli `AwsEc2VpcPeeringConnection` attributi, consulta AwsEc2VpcPeeringConnectionDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi del AWS Security Finding Format (ASFF) per le risorse. `AwsEcr`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsEcrContainerImage

L'`AwsEcrContainerImage`oggetto fornisce informazioni su un'immagine Amazon ECR.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcrContainerImage`oggetto. Per visualizzare le descrizioni degli `AwsEcrContainerImage` attributi, consulta AwsEcrContainerImageDetailsl'AWS Security Hub API Reference.

Esempio

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
```

```
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

L'`AwsEcrRepository`oggetto fornisce informazioni su un repository Amazon Elastic Container Registry.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcrRepository`oggetto. Per visualizzare le descrizioni degli `AwsEcrRepository` attributi, consulta AwsEcrRepositoryDetailsl'AWS Security Hub API Reference.

Esempio

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi del AWS Security Finding Format (ASFF) per le risorse. `AwsEcs`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsEcsCluster

L'`AwsEcsCluster`oggetto fornisce dettagli su un cluster Amazon Elastic Container Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcsCluster`oggetto. Per visualizzare le descrizioni degli `AwsEcsCluster` attributi, consulta AwsEcsClusterDetailsl'AWS Security Hub API Reference.

Esempio

```
    "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

L'`AwsEcsContainer`oggetto contiene dettagli su un contenitore Amazon ECS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcsContainer`oggetto. Per visualizzare le descrizioni degli `AwsEcsContainer` attributi, consulta AwsEcsContainerDetailsl'AWS Security Hub API Reference.

Esempio

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
```

```
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

L'`AwsEcsService`oggetto fornisce dettagli su un servizio all'interno di un cluster Amazon ECS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcsService`oggetto. Per visualizzare le descrizioni degli `AwsEcsService` attributi, consulta AwsEcsServiceDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEcsTask`oggetto fornisce dettagli su un'attività di Amazon ECS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcsTask`oggetto. Per visualizzare le descrizioni degli `AwsEcsTask` attributi, consulta AwsEcsTaskl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEcsTaskDefinition`oggetto contiene dettagli sulla definizione di un'attività. Una definizione di attività descrive le definizioni di contenitore e volume di un'attività di Amazon Elastic Container Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcsTaskDefinition`oggetto. Per visualizzare le descrizioni degli `AwsEcsTaskDefinition` attributi, consulta AwsEcsTaskDefinitionDetailsl'AWS Security Hub API Reference.

Esempio

```
    "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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi del AWS Security Finding Format (ASFF) per le `AwsEfs` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsEfsAccessPoint

L'`AwsEfsAccessPoint`oggetto fornisce dettagli sui file archiviati in Amazon Elastic File System.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEfsAccessPoint`oggetto. Per visualizzare le descrizioni degli `AwsEfsAccessPoint` attributi, consulta AwsEfsAccessPointDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi del AWS Security Finding Format (ASFF) per le `AwsEks` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsEksCluster

L'`AwsEksCluster`oggetto fornisce dettagli su un cluster Amazon EKS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEksCluster`oggetto. Per visualizzare le descrizioni degli `AwsEksCluster` attributi, consulta AwsEksClusterDetailsl'AWS Security Hub API Reference.

Esempio

```
{
  "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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsElasticBeanstalk`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsElasticBeanstalkEnvironment

L'`AwsElasticBeanstalkEnvironment`oggetto contiene dettagli su un AWS Elastic Beanstalk ambiente.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsElasticBeanstalkEnvironment`oggetto. Per visualizzare le descrizioni degli `AwsElasticBeanstalkEnvironment` attributi, consulta AwsElasticBeanstalkEnvironmentDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsElasticSearch` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsElasticSearchDomain

L'`AwsElasticSearchDomain`oggetto fornisce dettagli su un dominio Amazon OpenSearch Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsElasticSearchDomain`oggetto. Per visualizzare le descrizioni degli `AwsElasticSearchDomain` attributi, consulta AwsElasticSearchDomainDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsElb`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsElbLoadBalancer

L'`AwsElbLoadBalancer`oggetto contiene dettagli su un Classic Load Balancer.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsElbLoadBalancer`oggetto. Per visualizzare le descrizioni degli `AwsElbLoadBalancer` attributi, consulta AwsElbLoadBalancerDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'oggetto `AwsElbv2LoadBalancer` fornisce informazioni su un bilanciamento del carico.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsElbv2LoadBalancer`oggetto. Per visualizzare le descrizioni degli `AwsElbv2LoadBalancer` attributi, consulta AwsElbv2LoadBalancerDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsEventBridge` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsEventSchemasRegistry

L'`AwsEventSchemasRegistry`oggetto fornisce informazioni su un registro di EventBridge schemi Amazon. Uno schema definisce la struttura degli eventi a cui vengono inviati EventBridge. I registri degli schemi sono contenitori che raccolgono e raggruppano logicamente gli schemi.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsEventSchemasRegistry` Per visualizzare le descrizioni degli `AwsEventSchemasRegistry` attributi, consulta AwsEventSchemasRegistryl'AWS Security Hub API Reference.

Esempio

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

L'`AwsEventsEndpoint`oggetto fornisce informazioni su un endpoint EventBridge globale Amazon. L'endpoint può migliorare la disponibilità dell'applicazione rendendola Regional-fault tollerante.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsEventsEndpoint` Per visualizzare le descrizioni degli `AwsEventsEndpoint` attributi, consulta AwsEventsEndpointDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsEventsEventbus`oggetto fornisce informazioni su un endpoint EventBridge globale Amazon. L'endpoint può migliorare la disponibilità dell'applicazione rendendola Regional-fault tollerante.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsEventsEventbus` Per visualizzare le descrizioni degli `AwsEventsEventbus` attributi, consulta AwsEventsEventbusDetails l'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsGuardDuty` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsGuardDutyDetector

L'`AwsGuardDutyDetector`oggetto fornisce informazioni su un GuardDuty rilevatore Amazon. Un rilevatore è un oggetto che rappresenta il GuardDuty servizio. È necessario un rilevatore per GuardDuty diventare operativo.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsGuardDutyDetector`oggetto. Per visualizzare le descrizioni degli `AwsGuardDutyDetector` attributi, consulta AwsGuardDutyDetectorl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsIam` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsIamAccessKey

L'`AwsIamAccessKey`oggetto contiene dettagli su una chiave di accesso IAM correlata a un risultato.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsIamAccessKey`oggetto. Per visualizzare le descrizioni degli `AwsIamAccessKey` attributi, consulta AwsIamAccessKeyDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsIamGroup`oggetto contiene dettagli su un gruppo IAM.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsIamGroup`oggetto. Per visualizzare le descrizioni degli `AwsIamGroup` attributi, consulta AwsIamGroupDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsIamPolicy`oggetto rappresenta una politica di autorizzazioni IAM.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsIamPolicy`oggetto. Per visualizzare le descrizioni degli `AwsIamPolicy` attributi, consulta AwsIamPolicyDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsIamRole`oggetto contiene informazioni su un ruolo IAM, incluse tutte le politiche del ruolo.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsIamRole`oggetto. Per visualizzare le descrizioni degli `AwsIamRole` attributi, consulta AwsIamRoleDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsIamUser`oggetto fornisce informazioni su un utente.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsIamUser`oggetto. Per visualizzare le descrizioni degli `AwsIamUser` attributi, consulta AwsIamUserDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsKinesis`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsKinesisStream

L'`AwsKinesisStream`oggetto fornisce dettagli su Amazon Kinesis Data Streams.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsKinesisStream` Per visualizzare le descrizioni degli `AwsKinesisStream` attributi, consulta AwsKinesisStreamDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsKms` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsKmsKey

L'`AwsKmsKey`oggetto fornisce dettagli su un AWS KMS key.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsKmsKey`oggetto. Per visualizzare le descrizioni degli `AwsKmsKey` attributi, consulta AwsKmsKeyDetailsl'AWS Security Hub API Reference.

Esempio

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
```

```
                    "KeyRotationStatus": boolean,
                    "KeyState": "string",
                    "Origin": "string"
                }
```

AwsLambda

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsLambda`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsLambdaFunction

L'`AwsLambdaFunction`oggetto fornisce dettagli sulla configurazione di una funzione Lambda.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsLambdaFunction`oggetto. Per visualizzare le descrizioni degli `AwsLambdaFunction` attributi, consulta AwsLambdaFunctionDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsLambdaLayerVersion`oggetto fornisce dettagli su una versione del layer Lambda.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsLambdaLayerVersion`oggetto. Per visualizzare le descrizioni degli `AwsLambdaLayerVersion` attributi, consulta AwsLambdaLayerVersionDetailsl'AWS Security Hub API Reference.

Esempio

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
```

```
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsMsk`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsMskCluster

L'`AwsMskCluster`oggetto fornisce informazioni su un cluster Amazon Managed Streaming for Apache Kafka (Amazon MSK).

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsMskCluster` Per visualizzare le descrizioni degli `AwsMskCluster` attributi, consulta AwsMskClusterDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsNetworkFirewall` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsNetworkFirewallFirewall

L'`AwsNetworkFirewallFirewall`oggetto contiene dettagli su un AWS Network Firewall firewall.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsNetworkFirewallFirewall`oggetto. Per visualizzare le descrizioni degli `AwsNetworkFirewallFirewall` attributi, consulta AwsNetworkFirewallFirewallDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsNetworkFirewallFirewallPolicy`oggetto fornisce dettagli su una politica del firewall. Una politica firewall definisce il comportamento di un firewall di rete.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsNetworkFirewallFirewallPolicy`oggetto. Per visualizzare le descrizioni degli `AwsNetworkFirewallFirewallPolicy` attributi, consulta AwsNetworkFirewallFirewallPolicyDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsNetworkFirewallRuleGroup`oggetto fornisce dettagli su un gruppo di AWS Network Firewall regole. I gruppi di regole vengono utilizzati per ispezionare e controllare il traffico di rete. I gruppi di regole stateless si applicano ai singoli pacchetti. I gruppi di regole con stato si applicano ai pacchetti nel contesto del relativo flusso di traffico.

I gruppi di regole sono indicati nelle politiche del firewall.

Gli esempi seguenti mostrano il AWS Security Finding Format (ASFF) per l'`AwsNetworkFirewallRuleGroup`oggetto. Per visualizzare le descrizioni degli `AwsNetworkFirewallRuleGroup` attributi, consulta AwsNetworkFirewallRuleGroupDetailsl'AWS Security Hub API Reference.

Esempio: gruppo di regole stateless

```
"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"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Esempio: gruppo di regole stateful

```
"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"
                         }
                     ]
                 }
             ]
         }
    }
}
```

Di seguito è riportato un elenco di esempi di valori validi per `AwsNetworkFirewallRuleGroup` gli attributi:

- `Action`

  Valori validi: `PASS` | `DROP` | `ALERT`

- `Protocol`

  Valori validi: `IP` `TCP` | `UDP` | `ICMP` | `HTTP` | `FTP` | `TLS` `SMB` | `DNS` | `DCERPC` | `SSH` | `SMTP` | `IMAP` | `MSN` | `KRB5` | `IKEV2` | `TFTP` | `NTP` | `DHCP`

- `Flags`

  Valori validi: `FIN` | `SYN` | `RST` | `PSH` | `ACK` | `URG` | `ECE` | `CWR`

- `Masks`

  Valori validi: `FIN` | `SYN` | `RST` | `PSH` | `ACK` | `URG` | `ECE` | `CWR`

AwsOpenSearchService risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsOpenSearchService` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsOpenSearchServiceDomain

L'`AwsOpenSearchServiceDomain`oggetto contiene informazioni su un dominio Amazon OpenSearch Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsOpenSearchServiceDomain`oggetto. Per visualizzare le descrizioni degli `AwsOpenSearchServiceDomain` attributi, consulta AwsOpenSearchServiceDomainDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi del AWS Security Finding Format (ASFF) per le risorse. `AwsRds`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsRdsDbCluster

L'`AwsRdsDbCluster`oggetto fornisce dettagli su un cluster di database Amazon RDS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsRdsDbCluster`oggetto. Per visualizzare le descrizioni degli `AwsRdsDbCluster` attributi, consulta AwsRdsDbClusterDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsRdsDbClusterSnapshot`oggetto contiene informazioni su uno snapshot del cluster Amazon RDS DB.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsRdsDbClusterSnapshot` Per visualizzare le descrizioni degli `AwsRdsDbClusterSnapshot` attributi, consulta AwsRdsDbClusterSnapshotDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsRdsDbInstance`oggetto fornisce dettagli su un'istanza database Amazon RDS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsRdsDbInstance`oggetto. Per visualizzare le descrizioni degli `AwsRdsDbInstance` attributi, consulta AwsRdsDbInstanceDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsRdsDbSecurityGroup`oggetto contiene informazioni su un Amazon Relational Database Service

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsRdsDbSecurityGroup`oggetto. Per visualizzare le descrizioni degli `AwsRdsDbSecurityGroup` attributi, consulta AwsRdsDbSecurityGroupDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsRdsDbSnapshot`oggetto contiene dettagli su uno snapshot del cluster Amazon RDS DB.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsRdsDbSnapshot` Per visualizzare le descrizioni degli `AwsRdsDbSnapshot` attributi, consulta AwsRdsDbSnapshotDetails l'AWS Security Hub API Reference.

Esempio

```
"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

`AwsRdsEventSubscription`Contiene dettagli su un abbonamento per la notifica di eventi RDS. L'abbonamento consente a RDS di pubblicare eventi su un argomento SNS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsRdsEventSubscription` Per visualizzare le descrizioni degli `AwsRdsEventSubscription` attributi, consulta AwsRdsEventSubscriptionDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi del AWS Security Finding Format (ASFF) per le risorse. `AwsRedshift`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsRedshiftCluster

L'`AwsRedshiftCluster`oggetto contiene dettagli su un cluster Amazon Redshift.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsRedshiftCluster`oggetto. Per visualizzare le descrizioni degli `AwsRedshiftCluster` attributi, consulta AwsRedshiftClusterDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsRoute53` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsRoute53HostedZone

L'`AwsRoute53HostedZone`oggetto fornisce informazioni su una zona ospitata di Amazon Route 53, inclusi i quattro name server assegnati alla zona ospitata. Una zona ospitata rappresenta una raccolta di record che possono essere gestiti insieme, appartenenti a un unico nome di dominio principale.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsRoute53HostedZone`oggetto. Per visualizzare le descrizioni degli `AwsRoute53HostedZone` attributi, consulta AwsRoute53HostedZoneDetailsl'AWS Security Hub API Reference.

Esempio

```
"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"
        }
    ]
}
```

AWS 3 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsS3`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsS3AccessPoint

`AwsS3AccessPoint`fornisce informazioni su un punto di accesso Amazon S3. I punti di accesso S3 sono endpoint di rete denominati collegati ai bucket S3 che è possibile utilizzare per eseguire operazioni sugli oggetti S3.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsS3AccessPoint` Per visualizzare le descrizioni degli `AwsS3AccessPoint` attributi, consulta AwsS3AccessPointDetailsl'AWS Security Hub API Reference.

Esempio

```
"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`fornisce informazioni sulla configurazione del blocco di accesso pubblico di Amazon S3 per gli account.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsS3AccountPublicAccessBlock`oggetto. Per visualizzare le descrizioni degli `AwsS3AccountPublicAccessBlock` attributi, consulta AwsS3AccountPublicAccessBlockDetailsl'AWS Security Hub API Reference.

Esempio

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

L'`AwsS3Bucket`oggetto fornisce dettagli su un bucket Amazon S3.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsS3Bucket` Per visualizzare le descrizioni degli `AwsS3Bucket` attributi, consulta AwsS3BucketDetailsl'AWS Security Hub API Reference.

Esempio

```
"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"
                }
            }
        ]
     }
}
```

Oggetto AWS S3

L'`AwsS3Object`oggetto fornisce informazioni su un oggetto Amazon S3.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsS3Object`oggetto. Per visualizzare le descrizioni degli `AwsS3Object` attributi, consulta AwsS3ObjectDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsSageMaker` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsSageMakerNotebookInstance

L'`AwsSageMakerNotebookInstance`oggetto fornisce informazioni su un'istanza di notebook Amazon SageMaker AI, che è un'istanza di calcolo di machine learning che esegue l'app Jupyter Notebook.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsSageMakerNotebookInstance` Per visualizzare le descrizioni degli `AwsSageMakerNotebookInstance` attributi, consulta AwsSageMakerNotebookInstanceDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsSecretsManager` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsSecretsManagerSecret

L'`AwsSecretsManagerSecret`oggetto fornisce dettagli su un segreto di Secrets Manager.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsSecretsManagerSecret`oggetto. Per visualizzare le descrizioni degli `AwsSecretsManagerSecret` attributi, consulta AwsSecretsManagerSecretDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi del AWS Security Finding Format (ASFF) per le risorse. `AwsSns`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsSnsTopic

L'`AwsSnsTopic`oggetto contiene dettagli su un argomento di Amazon Simple Notification Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsSnsTopic`oggetto. Per visualizzare le descrizioni degli `AwsSnsTopic` attributi, consulta AwsSnsTopicDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi del AWS Security Finding Format (ASFF) per le risorse. `AwsSqs`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsSqsQueue

L'`AwsSqsQueue`oggetto contiene informazioni su una coda di Amazon Simple Queue Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsSqsQueue` Per visualizzare le descrizioni degli `AwsSqsQueue` attributi, consulta AwsSqsQueueDetailsl'AWS Security Hub API Reference.

Esempio

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le risorse. `AwsSsm`

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsSsmPatchCompliance

L'`AwsSsmPatchCompliance`oggetto fornisce informazioni sullo stato di una patch su un'istanza in base alla linea di base della patch utilizzata per applicare la patch all'istanza.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsSsmPatchCompliance`oggetto. Per visualizzare le descrizioni degli `AwsSsmPatchCompliance` attributi, consulta AwsSsmPatchComplianceDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsStepFunctions` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsStepFunctionStateMachine

L'`AwsStepFunctionStateMachine`oggetto fornisce informazioni su una macchina a AWS Step Functions stati, che è un flusso di lavoro costituito da una serie di passaggi basati sugli eventi.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsStepFunctionStateMachine` Per visualizzare le descrizioni degli `AwsStepFunctionStateMachine` attributi, consulta AwsStepFunctionStateMachinel'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsWaf` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsWafRateBasedRule

L'`AwsWafRateBasedRule`oggetto contiene dettagli su una regola AWS WAF basata sulla tariffa per le risorse globali. Una regola AWS WAF basata sulla tariffa fornisce impostazioni per indicare quando consentire, bloccare o contare una richiesta. Rate-based le regole includono il numero di richieste che arrivano in un determinato periodo di tempo.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsWafRateBasedRule`oggetto. Per visualizzare le descrizioni degli `AwsWafRateBasedRule` attributi, consulta AwsWafRateBasedRuleDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsWafRegionalRateBasedRule`oggetto contiene dettagli su una regola basata sulle tariffe per le risorse regionali. Una regola basata sulla tariffa fornisce impostazioni per indicare quando consentire, bloccare o contare una richiesta. Rate-based le regole includono il numero di richieste che arrivano in un determinato periodo di tempo.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsWafRegionalRateBasedRule`oggetto. Per visualizzare le descrizioni degli `AwsWafRegionalRateBasedRule` attributi, consulta AwsWafRegionalRateBasedRuleDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsWafRegionalRule`oggetto fornisce dettagli su una regola AWS WAF regionale. Questa regola identifica le richieste Web che desideri consentire, bloccare o contare.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsWafRegionalRule`oggetto. Per visualizzare le descrizioni degli `AwsWafRegionalRule` attributi, consulta AwsWafRegionalRuleDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsWafRegionalRuleGroup`oggetto fornisce dettagli su un gruppo di regole AWS WAF regionali. Un gruppo di regole è una raccolta di regole predefinite che si aggiungono a un elenco di controllo degli accessi Web (Web ACL).

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsWafRegionalRuleGroup` Per visualizzare le descrizioni degli `AwsWafRegionalRuleGroup` attributi, consulta AwsWafRegionalRuleGroupDetailsl'AWS Security Hub API Reference.

Esempio

```
"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`fornisce dettagli su un elenco AWS WAF regionale di controllo degli accessi Web (Web ACL). Un ACL Web contiene le regole che identificano le richieste che si desidera consentire, bloccare o contare.

Di seguito è riportato un esempio di `AwsWafRegionalWebAcl` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayV2Stage` attributi, consulta AwsWafRegionalWebAclDetailsl'AWS Security Hub API Reference.

Esempio

```
"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`fornisce informazioni su una AWS WAF regola. Una AWS WAF regola identifica le richieste Web che desideri consentire, bloccare o contare.

Di seguito è riportato un esempio di `AwsWafRule` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayV2Stage` attributi, consulta AwsWafRuleDetailsl'AWS Security Hub API Reference.

Esempio

```
"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`fornisce informazioni su un gruppo di AWS WAF regole. Un gruppo di AWS WAF regole è una raccolta di regole predefinite che si aggiungono a un elenco di controllo degli accessi Web (Web ACL).

Di seguito è riportato un esempio `AwsWafRuleGroup` trovato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayV2Stage` attributi, consulta AwsWafRuleGroupDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsWafv2RuleGroup`oggetto fornisce dettagli su un gruppo di regole AWS WAF V2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsWafv2RuleGroup`oggetto. Per visualizzare le descrizioni degli `AwsWafv2RuleGroup` attributi, consulta AwsWafv2RuleGroupDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsWafWebAcl`oggetto fornisce dettagli su un ACL AWS WAF web.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsWafWebAcl`oggetto. Per visualizzare le descrizioni degli `AwsWafWebAcl` attributi, consulta AwsWafWebAclDetailsl'AWS Security Hub API Reference.

Esempio

```
"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

L'`AwsWafv2WebAcl`oggetto fornisce dettagli su un ACL Web AWS WAF V2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. `AwsWafv2WebAcl` Per visualizzare le descrizioni degli `AwsWafv2WebAcl` attributi, consulta AwsWafv2WebAclDetailsl'AWS Security Hub API Reference.

Esempio

```
"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 risorse in ASFF

Di seguito sono riportati alcuni esempi della sintassi ASFF (AWS Security Finding Format) per le `AwsXray` risorse.

AWS Security Hub CSPM normalizza i risultati provenienti da varie fonti in ASFF. Per informazioni di base su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

AwsXrayEncryptionConfig

L'`AwsXrayEncryptionConfig`oggetto contiene informazioni sulla configurazione di crittografia per AWS X-Ray.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsXrayEncryptionConfig`oggetto. Per visualizzare le descrizioni degli `AwsXrayEncryptionConfig` attributi, consulta AwsXrayEncryptionConfigDetailsl'AWS Security Hub API Reference.

Esempio

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

CodeRepository oggetto in ASFF

L'`CodeRepository`oggetto fornisce informazioni su un repository di codice esterno collegato alle AWS risorse e configurato Amazon Inspector per la scansione delle vulnerabilità.

L'esempio seguente mostra la sintassi ASFF (AWS Security Finding Format) per l'oggetto. `CodeRepository` Per visualizzare le descrizioni degli `CodeRepository` attributi, consulta l'AWS Security Hub API CodeRepositoryDetailsReference. Per informazioni di base su ASFF, vedereAWS Formato ASFF (Security Finding Format).

Esempio

```
"CodeRepository": {
    "ProviderType": "GITLAB_SELF_MANAGED",
    "ProjectName": "projectName",
    "CodeSecurityIntegrationArn": "arn:aws:inspector2:us-
east-1:123456789012:codesecurity-integration/00000000-0000-0000-0000-000000000000"
}
```

Contenitore oggetto in ASFF

L'esempio seguente mostra la sintassi ASFF (AWS Security Finding Format) per l'`Container`oggetto. Per visualizzare le descrizioni degli `Container` attributi, consulta l'AWS Security Hub API ContainerDetailsReference. Per informazioni di base su ASFF, vedereAWS Formato ASFF (Security Finding Format).

Esempio

```
"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"
    }]
}
```

Altro oggetto in ASFF

Nel AWS Security Finding Format (ASFF), l'`Other`oggetto specifica campi e valori personalizzati. Per ulteriori informazioni su ASFF, vedere. AWS Formato ASFF (Security Finding Format)

Utilizzando l'`Other`oggetto, è possibile specificare campi e valori personalizzati per una risorsa. È possibile utilizzare l'`Other`oggetto nei seguenti casi:

- Il tipo di risorsa non ha un `Details` oggetto corrispondente. Per specificare i dettagli di una risorsa, utilizzate l'`Other`oggetto.

- L'`Details`oggetto per il tipo di risorsa non include tutti gli attributi che si desidera specificare. In questo caso, utilizzate l'`Details`oggetto relativo al tipo di risorsa per specificare gli attributi disponibili. Utilizzate l'`Other`oggetto per specificare gli attributi che non sono presenti nell'oggetto specifico del tipo`Details`.
- Il tipo di risorsa non è uno dei tipi forniti. In questo caso, `Resource.Type` impostate `Other` e utilizzate l'`Other`oggetto per specificare i dettagli.

Tipo: mappa di un massimo di 50 coppie chiave-valore

Ogni coppia chiave/valore deve soddisfare i seguenti requisiti.

- La chiave deve contenere meno di 128 caratteri.
- Il valore deve contenere meno di 1.024 caratteri.

Visualizzazione degli approfondimenti in Security Hub CSPM

In AWS Security Hub CSPM, un'analisi è una raccolta di risultati correlati. Un'analisi può identificare un'area di sicurezza specifica che richiede attenzione e intervento. Ad esempio, un'informazione dettagliata potrebbe indicare le istanze EC2 con risultati che rilevano procedure di sicurezza inadeguate. Un'informazione dettagliata riunisce i risultati di tutti i provider di ricerca.

Ogni informazione dettagliata è definita da un gruppo per istruzione e filtri facoltativi. Il gruppo per istruzione indica come raggruppare i risultati corrispondenti e identifica il tipo di elemento a cui si applica l'informazione dettagliata. Ad esempio, se un'informazione dettagliata è raggruppata per identificatore di risorsa, l'informazione dettagliata produce un elenco di identificatori di risorse. I filtri opzionali identificano i risultati corrispondenti all'analisi. Ad esempio, potresti voler visualizzare solo i risultati di fornitori specifici o i risultati associati a tipi specifici di risorse.

Security Hub CSPM offre diverse informazioni gestite integrate. Non è possibile modificare o eliminare le informazioni gestite. Per tenere traccia dei problemi di sicurezza specifici del tuo AWS ambiente e del tuo utilizzo, puoi creare approfondimenti personalizzati.

La pagina Insights sulla console CSPM AWS di Security Hub mostra l'elenco degli approfondimenti disponibili.

Per impostazione predefinita, l'elenco mostra sia gli approfondimenti gestiti che quelli personalizzati. Per filtrare l'elenco di approfondimenti in base al tipo di analisi, scegli il tipo di analisi dal menu a discesa accanto al campo del filtro.

- Per visualizzare tutti gli approfondimenti disponibili, scegli Tutti gli approfondimenti. Questa è l'opzione predefinita.
- Per visualizzare solo gli approfondimenti gestiti, scegli Security Hub CSPM managed insights.
- Per visualizzare solo approfondimenti personalizzati, scegli Informazioni personalizzate.

Puoi anche filtrare l'elenco degli approfondimenti in base al nome dell'approfondimento. A tale scopo, nel campo del filtro, digita il testo da utilizzare per filtrare l'elenco. Il filtro non fa distinzione tra maiuscole e minuscole. Il filtro cerca gli approfondimenti che contengono il testo in un punto qualsiasi del nome dell'approfondimento.

Un'analisi restituisce risultati solo se sono state abilitate integrazioni o standard che producono risultati corrispondenti. Ad esempio, il managed insight 29. Le migliori risorse in base al numero di controlli CIS non riusciti restituiscono risultati solo se si abilita una versione dello standard Center for Internet Security (CIS) AWS Foundations Benchmark.

Revisione e azione in base agli approfondimenti in Security Hub CSPM

Per ogni analisi, AWS Security Hub CSPM determina innanzitutto i risultati che corrispondono ai criteri di filtro, quindi utilizza l'attributo grouping per raggruppare i risultati corrispondenti.

Dalla pagina Insights sulla console, puoi visualizzare i risultati e le scoperte e intervenire in base a essi.

Se abiliti l'aggregazione interregionale, i risultati per gli approfondimenti gestiti (quando hai effettuato l'accesso alla regione di aggregazione) includono i risultati della regione di aggregazione e delle regioni collegate. I risultati degli approfondimenti personalizzati, se gli approfondimenti non vengono filtrati per regione, includono anche i risultati della regione di aggregazione e delle regioni collegate (quando hai effettuato l'accesso alla regione di aggregazione). In altre regioni, i risultati degli approfondimenti riguardano solo quella regione.

Per informazioni sulla configurazione dell'aggregazione interregionale, consulta. the section called "Aggregazione dei dati tra le regioni"

Visualizzazione e azione in base ai risultati delle informazioni

I risultati di informazione dettagliata sono costituiti dall'elenco raggruppato dei risultati dell'informazione dettagliata. Ad esempio, se l'approfondimento è raggruppato per identificatori di risorse, i risultati dell'analisi sono l'elenco degli identificatori delle risorse. Ogni voce nell'elenco dei risultati indica il numero di risultati corrispondenti per la voce.

Se i risultati sono raggruppati per identificatore di risorsa o tipo di risorsa, i risultati includono tutte le risorse nei risultati corrispondenti. Sono incluse le risorse di tipo diverso da quello specificato nei criteri di filtro. Ad esempio, un insight identifica i risultati associati ai bucket S3. Se un risultato corrispondente contiene sia una risorsa bucket S3 che una risorsa chiave di accesso IAM, i risultati dell'analisi includono entrambe le risorse.

Sulla console Security Hub CSPM, l'elenco dei risultati è ordinato dal maggior numero di risultati corrispondenti al minor numero di risultati corrispondenti. Security Hub CSPM può visualizzare solo 100 risultati. Se sono presenti più di 100 valori di raggruppamento, vengono visualizzati solo i primi 100.

Oltre all'elenco dei risultati, i risultati dell'informazione dettagliata visualizzano una serie di grafici riepilogativi con il numero di risultati corrispondenti per gli attributi seguenti.

- Etichetta di gravità: numero di risultati per ciascuna etichetta di gravità
- Account AWS ID: i primi cinque ID di account per i risultati corrispondenti
- Tipo di risorsa: i cinque principali tipi di risorse per i risultati corrispondenti
- ID risorsa: i primi cinque ID di risorsa per i risultati corrispondenti
- Nome del prodotto: i cinque principali fornitori di ricerca per i risultati corrispondenti

Se sono state configurate azioni personalizzate, puoi inviare i risultati selezionati a un'azione personalizzata. L'azione deve essere associata a una CloudWatch regola Amazon per il tipo di `Security Hub Insight Results` evento. Per ulteriori informazioni, consulta the section called "Risposta e riparazione automatiche". Se non hai configurato azioni personalizzate, il menu Azioni è disabilitato.

Security Hub CSPM console

Per visualizzare e intervenire sui risultati di Insight (console)

1. Aprire la console AWS Security Hub CSPM all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, seleziona Informazioni dettagliate.
3. Per visualizzare l'elenco dei risultati di informazione dettagliata, scegliere il nome dell'informazione dettagliata.
4. Selezionare la casella di controllo per ogni risultato da inviare all'azione personalizzata.
5. Dal menu Actions (Azioni) scegliere l'azione personalizzata.

Security Hub CSPM API, AWS CLI

Per visualizzare e intervenire sui risultati di Insights (API,) AWS CLI

Per visualizzare i risultati degli approfondimenti, utilizza il >GetInsightResults funzionamento dell'API CSPM di Security Hub. Se usi il AWS CLI, esegui il comando. get-insight-results

Per identificare l'insight per cui restituire i risultati, è necessario l'insight ARN. Per ottenere gli ARN di insight per approfondimenti personalizzati, utilizza l'operazione `GetInsights` API o il get-insight-results comando.

L'esempio seguente recupera i risultati per l'insight specificato. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

Per informazioni su come creare azioni personalizzate a livello di programmazione, vedere. Utilizzo di azioni personalizzate per inviare risultati e approfondimenti a EventBridge

Visualizzazione e azione in base ai risultati di Insight (console)

Da un elenco dei risultati di Insight sulla console Security Hub CSPM, è possibile visualizzare l'elenco dei risultati per ciascun risultato.

Per visualizzare e intervenire sui risultati di Insight (console)

1. Aprire la console AWS Security Hub CSPM all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, seleziona Informazioni dettagliate.
3. Per visualizzare l'elenco dei risultati di informazione dettagliata, scegliere il nome dell'informazione dettagliata.
4. Per visualizzare l'elenco dei risultati per un risultato di informazione dettagliata, scegliere la voce dall'elenco dei risultati. L'elenco dei risultati mostra i risultati attivi per il risultato di informazioni dettagliate selezionato che hanno uno stato del flusso di lavoro `NEW` o `NOTIFIED`.

Dall'elenco dei risultati, è possibile eseguire le seguenti azioni:

- Filtraggio dei risultati in Security Hub CSPM
- Revisione dei dettagli e della cronologia dei risultati
- Impostazione dello stato del flusso di lavoro dei risultati in Security Hub CSPM
- Invio dei risultati a un'azione CSPM personalizzata di Security Hub

Informazioni gestite in Security Hub CSPM

AWSSecurity Hub CSPM fornisce diverse informazioni gestite.

Non puoi modificare o eliminare le informazioni gestite da Security Hub CSPM. Puoi visualizzare e agire in merito ai risultati e ai risultati di informazione dettagliata. Puoi anche utilizzare un'informazione dettagliata gestita come base per una nuova informazione dettagliata personalizzata.

Come tutte le informazioni dettagliate, un'informazione dettagliata gestita restituisce i risultati solo se sono state abilitate le integrazioni di prodotti o standard di sicurezza che producono risultati corrispondenti.

Per gli approfondimenti raggruppati per identificatore di risorsa, i risultati includono gli identificatori di tutte le risorse nei risultati corrispondenti. Ciò include le risorse che hanno un tipo diverso dal tipo di risorsa indicato nei criteri di filtro. Ad esempio, insight 2 nell'elenco seguente identifica i risultati associati ai bucket Amazon S3. Se un risultato corrispondente contiene sia una risorsa bucket S3 che una risorsa chiave di accesso IAM, i risultati dell'analisi includono entrambe le risorse.

Security Hub CSPM offre attualmente le seguenti informazioni gestite:

1. AWSrisorse con il maggior numero di risultati

   ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

   Raggruppati per: identificatore di risorse

   Ricerca dei filtri:

   - Lo stato del record è `ACTIVE`
   - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

2. Bucket S3 con autorizzazioni di lettura o scrittura pubblica

   ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

Raggruppati per: identificatore di risorse

Ricerca dei filtri:

- Il tipo inizia con `Effects/Data Exposure`
- Il tipo di risorsa è `AwsS3Bucket`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

3. AMI che generano la maggior parte dei risultati

   ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

   Raggruppati per: ID dell'immagine dell'istanza EC2

   Ricerca dei filtri:

   - Il tipo di risorsa è `AwsEc2Instance`
   - Lo stato del record è `ACTIVE`
   - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

4. Istanze EC2 coinvolte in TTPs (Tactics, Techniques, and Procedures) note

   ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

   Raggruppati per: Resource ID

   Ricerca dei filtri:

   - Il tipo inizia con `TTPs`
   - Il tipo di risorsa è `AwsEc2Instance`
   - Lo stato del record è `ACTIVE`
   - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

5. AWSpresidi con attività sospette relative alle chiavi di accesso

   ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

   Raggruppati per: nome principale della chiave di accesso IAM

   Ricerca dei filtri:

   - Il tipo di risorsa è `AwsIamAccessKey`

- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

6. AWSrisorse: istanze che non soddisfano gli standard di sicurezza/le migliori pratiche

   ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

   Raggruppati per: Resource ID

   Ricerca dei filtri:

   - Il tipo è `Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices`
   - Lo stato del record è `ACTIVE`
   - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

7. AWSrisorse associate alla potenziale esfiltrazione di dati

   ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

   Raggruppati per:: Resource ID

   Ricerca dei filtri:

   - Il tipo inizia con Effects/Data Exfiltration/
   - Lo stato del record è `ACTIVE`
   - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

8. AWSrisorse associate al consumo non autorizzato di risorse

   ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

   Raggruppate per: Resource ID

   Ricerca dei filtri:

   - Il tipo inizia con `Effects/Resource Consumption`
   - Lo stato del record è `ACTIVE`
   - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

9. Bucket S3 che non soddisfano standard di sicurezza o best practice

   ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo di risorsa è `AwsS3Bucket`
- Il tipo è `Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

10. Bucket S3 con dati sensibili

    ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - Il tipo di risorsa è `AwsS3Bucket`
    - Il tipo inizia con `Sensitive Data Identifications/`
    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

11. Credenziali che possono essere state divulgate

    ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - Il tipo inizia con `Sensitive Data Identifications/Passwords/`
    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

12. Istanze EC2 con patch di sicurezza mancanti per vulnerabilità importanti

    ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

- Il tipo inizia con `Software and Configuration Checks/Vulnerabilities/CVE`
- Il tipo di risorsa è `AwsEc2Instance`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

13. Istanze EC2 con comportamento insolito generale

    ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - Il tipo inizia con `Unusual Behaviors`
    - Il tipo di risorsa è `AwsEc2Instance`
    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

14. Istanze EC2 che dispongono di porte accessibili da Internet

    ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - Il tipo inizia con `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
    - Il tipo di risorsa è `AwsEc2Instance`
    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

15. Istanze EC2 che non soddisfano standard di sicurezza o best practice

    ARN: `arn:aws:securityhub:::insight/securityhub/default/19`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - Il tipo inizia con uno dei seguenti valori:

    - `Software and Configuration Checks/Industry and Regulatory Standards/`
    - `Software and Configuration Checks/AWSSecurity Best Practices`
  - Il tipo di risorsa è `AwsEc2Instance`
  - Lo stato del record è `ACTIVE`
  - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`
16. Istanze EC2 aperte a Internet

    ARN: `arn:aws:securityhub:::insight/securityhub/default/21`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

  - Il tipo inizia con `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
  - Il tipo di risorsa è `AwsEc2Instance`
  - Lo stato del record è `ACTIVE`
  - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`
17. Istanze EC2 associate a riconoscimento avversario

    ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

  - Il tipo inizia con TTPs/Discovery/Recon
  - Il tipo di risorsa è `AwsEc2Instance`
  - Lo stato del record è `ACTIVE`
  - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`
18. AWSrisorse associate al malware

    ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

    Raggruppate per: Resource ID

    Ricerca dei filtri:

- Il tipo inizia con uno dei seguenti valori:
  - `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`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

19. AWSrisorse associate ai problemi relativi alle criptovalute

    ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - Il tipo inizia con uno dei seguenti valori:
      - `Effects/Resource Consumption/Cryptocurrency`
      - `TTPs/Command and Control/CryptoCurrency`
    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

20. AWSrisorse con tentativi di accesso non autorizzati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/25`

    Raggruppate per: Resource ID

    Ricerca dei filtri:

    - Il tipo inizia con uno dei seguenti valori:
      - `TTPs/Command and Control/UnauthorizedAccess`
      - `TTPs/Initial Access/UnauthorizedAccess`
      - `Effects/Data Exfiltration/UnauthorizedAccess`
      - `Unusual Behaviors/User/UnauthorizedAccess`

    - `Effects/Resource Consumption/UnauthorizedAccess`
  - Lo stato del record è `ACTIVE`
  - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

21. Indicatori di intelligence delle minacce con la maggior parte delle occorrenze nell'ultima settimana

    ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

    Ricerca di filtri:

    - Creato negli ultimi 7 giorni

22. Principali account per numero di risultati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

    Raggruppati per: ID Account AWS

    Ricerca dei filtri:

    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

23. Principali prodotti per numero di risultati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

    Raggruppati per: Nome del prodotto

    Ricerca dei filtri:

    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

24. Gravità per numero di risultati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

    Raggruppati per: etichetta di severità

    Ricerca dei filtri:

    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

25. Principali bucket S3 per numero di risultati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - Il tipo di risorsa è `AwsS3Bucket`
    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

26. Principali istanze EC2 per numero di risultati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - Il tipo di risorsa è `AwsEc2Instance`
    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

27. Principali AMI per numero di risultati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

    Raggruppati per: ID dell'immagine dell'istanza EC2

    Ricerca dei filtri:

    - Il tipo di risorsa è `AwsEc2Instance`
    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

28. Principali utenti IAM per numero di risultati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/33`

    Raggruppati per: ID della chiave di accesso IAM

    Ricerca di filtri:

- Il tipo di risorsa è `AwsIamAccessKey`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

29. Principali risorse per numero di controlli CIS non riusciti

    ARN: `arn:aws:securityhub:::insight/securityhub/default/34`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - L'ID generatore inizia con `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
    - Aggiornato nell'ultimo giorno
    - Lo stato di conformità è `FAILED`
    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

30. Principali integrazioni per numero di risultati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/35`

    Raggruppato per: ARN del prodotto

    Ricerca dei filtri:

    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

31. Risorse con più controlli di sicurezza con esito negativo

    ARN: `arn:aws:securityhub:::insight/securityhub/default/36`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - Aggiornato nell'ultimo giorno
    - Lo stato di conformità è `FAILED`
    - Lo stato del record è `ACTIVE`

- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

32. Utenti IAM con attività sospette

    ARN: `arn:aws:securityhub:::insight/securityhub/default/37`

    Raggruppati per: utente IAM

    Ricerca dei filtri:

    - Il tipo di risorsa è `AwsIamUser`
    - Lo stato del record è `ACTIVE`
    - Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

33. Risorse con il maggior numero di AWS Health risultati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - `ProductName`è uguale `Health`

34. Risorse con il maggior numero di AWS Config risultati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/39`

    Raggruppati per: Resource ID

    Ricerca dei filtri:

    - `ProductName`è uguale `Config`

35. Applicazioni con il maggior numero di risultati

    ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

    Raggruppati per: ResourceApplicationArn

    Ricerca dei filtri:

    - `RecordState`è uguale `ACTIVE`
    - `Workflow.Status`è uguale o `NEW` `NOTIFIED`

Comprendere gli approfondimenti personalizzati in Security Hub CSPM

Oltre agli approfondimenti gestiti da AWS Security Hub CSPM, puoi creare approfondimenti personalizzati in Security Hub CSPM per tenere traccia dei problemi specifici del tuo ambiente. Gli approfondimenti personalizzati ti aiutano a tenere traccia di un sottoinsieme selezionato di problemi.

Ecco alcuni esempi di approfondimenti personalizzati che possono essere utili da configurare:

- Se possiedi un account amministratore, puoi impostare una panoramica personalizzata per tenere traccia dei risultati critici e di elevata gravità che riguardano gli account dei membri.
- Se ti affidi a un AWS servizio integrato specifico, puoi impostare una panoramica personalizzata per tenere traccia dei risultati critici e di elevata gravità di quel servizio.
- Se ti affidi a un'integrazione di terze parti, puoi impostare una panoramica personalizzata per tenere traccia dei risultati critici e di elevata gravità di quel prodotto integrato.

Puoi creare informazioni dettagliate personalizzate completamente nuove oppure iniziare da un'informazione dettagliata personalizzata o gestita già esistente.

Ogni analisi può essere configurata con le seguenti opzioni:

- Attributo di raggruppamento: l'attributo di raggruppamento determina quali elementi vengono visualizzati nell'elenco dei risultati di Insight. Ad esempio, se l'attributo di raggruppamento è Product name, i risultati di insight mostrano il numero di risultati associati a ciascun fornitore di risultati.
- Filtri opzionali: i filtri restringono i risultati corrispondenti alle informazioni.

  Un risultato è incluso nei risultati dell'approfondimento solo se corrisponde a tutti i filtri forniti. Ad esempio, se i filtri sono «Il nome del prodotto è GuardDuty" e «Il tipo di risorsa è `AwsS3Bucket` «, i risultati corrispondenti devono soddisfare entrambi questi criteri.

  Tuttavia, Security Hub CSPM applica la logica OR booleana ai filtri che utilizzano lo stesso attributo ma valori diversi. Ad esempio, se i filtri sono «Il nome del prodotto è GuardDuty" e «Il nome del prodotto è Amazon Inspector», un risultato corrisponde se è stato generato da Amazon o Amazon Inspector. GuardDuty

Se utilizzi l'identificatore o il tipo di risorsa come attributo di raggruppamento, i risultati di approfondimento includono tutte le risorse presenti nei risultati corrispondenti. L'elenco non è

limitato alle risorse che corrispondono a un filtro per tipo di risorsa. Ad esempio, un insight identifica i risultati associati ai bucket S3 e li raggruppa per identificatore di risorsa. Un risultato corrispondente contiene sia una risorsa bucket S3 che una risorsa chiave di accesso IAM. I risultati delle informazioni includono entrambe le risorse.

Se abiliti l'aggregazione interregionale e quindi crei un approfondimento personalizzato, l'approfondimento si applica ai risultati corrispondenti nella regione di aggregazione e nelle regioni collegate. L'eccezione è se le tue informazioni includono un filtro regionale.

Creazione di una panoramica personalizzata

In AWS Security Hub CSPM, è possibile utilizzare informazioni personalizzate per raccogliere una serie specifica di risultati e tenere traccia dei problemi specifici dell'ambiente. Per informazioni di base sugli approfondimenti personalizzati, consulta. Comprendere gli approfondimenti personalizzati in Security Hub CSPM

Scegli il tuo metodo preferito e segui i passaggi per creare una panoramica personalizzata in Security Hub CSPM

Security Hub CSPM console

Per creare una panoramica personalizzata (console)

1. Aprire la console AWS Security Hub CSPM all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, seleziona Informazioni dettagliate.
3. Scegliere Create insight (Crea informazione dettagliata).
4. Per selezionare l'attributo di raggruppamento per l'informazione dettagliata:
    a. Scegli la casella di ricerca per visualizzare le opzioni di filtro.
    b. Scegliere Group by (Raggruppa per).
    c. Seleziona l'attributo da utilizzare per raggruppare i risultati associati a questo approfondimento.
    d. Scegli Applica.
5. Facoltativamente, scegli eventuali filtri aggiuntivi da utilizzare per questo approfondimento. Per ogni filtro, definisci i criteri di filtro, quindi scegli Applica.
6. Scegliere Create insight (Crea informazione dettagliata).

7. Inserisci un nome Insight, quindi scegli Crea insight.

Security Hub CSPM API

Per creare un insight personalizzato (API)

1. Per creare un insight personalizzato, utilizza il CreateInsight funzionamento dell'API CSPM Security Hub. Se usi il AWS CLI, esegui il comando. create-insight
2. Compila il `Name` parametro con un nome per le tue informazioni personalizzate.
3. Compila il `Filters` parametro per specificare quali risultati includere nell'approfondimento.
4. Compila il `GroupByAttribute` parametro per specificare quale attributo viene utilizzato per raggruppare i risultati inclusi nell'insight.
5. Facoltativamente, compila il `SortCriteria` parametro per ordinare i risultati in base a un campo specifico.

L'esempio seguente crea una panoramica personalizzata che include risultati critici relativi al tipo di `AwsIamRole` risorsa. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

Per creare un insight personalizzato (PowerShell)

1. Utilizza il cmdlet `New-SHUBInsight`.
2. Compila il `Name` parametro con un nome per la tua panoramica personalizzata.
3. Compila il `Filter` parametro per specificare quali risultati includere nell'approfondimento.
4. Compila il `GroupByAttribute` parametro per specificare quale attributo viene utilizzato per raggruppare i risultati inclusi nell'insight.

Se hai abilitato l'aggregazione tra regioni e utilizzi questo cmdlet dalla regione di aggregazione, le informazioni si applicano ai risultati corrispondenti dell'aggregazione e delle regioni collegate.

Esempio

```
$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
```

Creazione di un insight personalizzato da un insight gestito (solo console)

Non è possibile salvare le modifiche o eliminare un insight gestito. Tuttavia, puoi utilizzare un insight gestito come base per un insight personalizzato. Questa è un'opzione disponibile solo sulla console Security Hub CSPM.

Per creare un insight personalizzato da un insight gestito (console)

1. Aprire la console AWS Security Hub CSPM all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, seleziona Informazioni dettagliate.
3. Scegliere l'informazione dettagliata gestita da utilizzare.
4. Modifica la configurazione di Insight secondo necessità.
   - Per modificare l'attributo utilizzato per raggruppare i risultati nell'informazione dettagliata:
     a. Per rimuovere il raggruppamento esistente, scegli la X accanto all'impostazione Raggruppa per impostazione.
     b. Scegli la barra di ricerca.
     c. Selezionare l'attributo da utilizzare per il raggruppamento.
     d. Scegli Applica.
   - Per rimuovere un filtro dall'insight, scegli la X cerchiata accanto al filtro.
   - Per aggiungere un filtro all'informazione dettagliata:
     a. Scegli la barra di ricerca.

b. Selezionare l'attributo e il valore da utilizzare come filtro.

c. Scegli Applica.

5. Al termine degli aggiornamenti, scegliere Create insight (Crea informazione dettagliata).
6. Quando richiesto, inserisci un nome Insight, quindi scegli Crea insight.

Modifica di un approfondimento personalizzato

È possibile modificare una panoramica personalizzata esistente per modificare il valore di raggruppamento e i filtri. Dopo aver apportato le modifiche, puoi salvare gli aggiornamenti nell'informazione dettagliata originale o salvare la versione aggiornata come una nuova informazione dettagliata.

In AWS Security Hub CSPM, è possibile utilizzare informazioni personalizzate per raccogliere una serie specifica di risultati e tenere traccia dei problemi specifici dell'ambiente. Per informazioni di base sugli approfondimenti personalizzati, consulta. Comprendere gli approfondimenti personalizzati in Security Hub CSPM

Per modificare un approfondimento personalizzato, scegli il tuo metodo preferito e segui le istruzioni.

Security Hub CSPM console

Per modificare un approfondimento personalizzato (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, seleziona Informazioni dettagliate.
3. Scegliere l'informazione dettagliata personalizzata da modificare.
4. Modifica la configurazione di Insight secondo necessità.

   - Per modificare l'attributo utilizzato per raggruppare i risultati nell'informazione dettagliata:
     a. Per rimuovere il raggruppamento esistente, scegli la X accanto all'impostazione Raggruppa per impostazione.
     b. Scegli la barra di ricerca.
     c. Selezionare l'attributo da utilizzare per il raggruppamento.
     d. Scegli Applica.
   - Per rimuovere un filtro dall'insight, scegli la X cerchiata accanto al filtro.

- Per aggiungere un filtro all'informazione dettagliata:
  a. Scegli la barra di ricerca.
  b. Selezionare l'attributo e il valore da utilizzare come filtro.
  c. Scegli Applica.

5. Al termine degli aggiornamenti, scegliere Save insight (Salva informazione dettagliata).
6. Quando richiesto, eseguire una delle operazioni seguenti:

   - Per aggiornare le informazioni esistenti in modo che riflettano le modifiche, scegli Aggiorna, ***<Insight_Name>*** quindi scegli Salva informazioni.
   - Per creare una nuova informazione dettagliata con gli aggiornamenti, scegliere Save new insight (Salva nuova informazione dettagliata). Immettere un Insight name (Nome informazione dettagliata), quindi scegliere Save insight (Salva informazione dettagliata).

Security Hub CSPM API

Per modificare un approfondimento personalizzato (API)

1. Utilizza il `UpdateInsight` funzionamento dell'API CSPM Security Hub. Se si utilizza il AWS CLI comando, eseguire il comando. update-insight
2. Per identificare le informazioni personalizzate che desideri aggiornare, fornisci l'Amazon Resource Name (ARN) dell'insight. Per ottenere l'ARN di un insight personalizzato, usa l'`GetInsights`operazione o il get-insights comando.
3. Aggiorna i `GroupByAttribute` parametri `NameFilters`, e se necessario.

L'esempio seguente aggiorna le informazioni dettagliate specificate. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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

Per modificare un insight personalizzato (PowerShell)

1. Utilizza il cmdlet `Update-SHUBInsight`.
2. Per identificare l'insight personalizzato, fornisci l'Amazon Resource Name (ARN) dell'insight. Per ottenere l'ARN di un insight personalizzato, usa il `Get-SHUBInsight` cmdlet.
3. Aggiorna i `GroupByAttribute` parametri `NameFilter`, e se necessario.

Esempio

```
$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"
```

Eliminazione di un insight personalizzato

In AWS Security Hub CSPM, è possibile utilizzare informazioni personalizzate per raccogliere una serie specifica di risultati e tenere traccia dei problemi specifici dell'ambiente. Per informazioni di base sugli approfondimenti personalizzati, consulta. Comprendere gli approfondimenti personalizzati in Security Hub CSPM

Per eliminare un approfondimento personalizzato, scegli il tuo metodo preferito e segui le istruzioni. Non puoi eliminare un insight gestito.

Security Hub CSPM console

Per eliminare un insight personalizzato (console)

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, seleziona Informazioni dettagliate.
3. Individuare l'informazione dettagliata personalizzata da eliminare.
4. Per maggiori informazioni, scegli l'icona Altre opzioni (i tre puntini nell'angolo in alto a destra della scheda).
5. Scegli Elimina.

Security Hub CSPM API

Per eliminare un insight personalizzato (API)

1. Utilizza il `DeleteInsight` funzionamento dell'API CSPM di Security Hub. Se si utilizza il AWS CLI comando, eseguire il comando. delete-insight
2. Per identificare l'insight personalizzato da eliminare, fornisci l'ARN dell'insight. Per ottenere l'ARN di un insight personalizzato, usa l'`GetInsights`operazione o get-insights il comando.

L'esempio seguente elimina l'insight specificato. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

PowerShell

Per eliminare un insight personalizzato () PowerShell

1. Utilizza il cmdlet `Remove-SHUBInsight`.
2. Per identificare l'insight personalizzato, fornisci l'ARN dell'insight. Per ottenere l'ARN di un insight personalizzato, usa il `Get-SHUBInsight` cmdlet.

Esempio

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Modifica e azione automatica dei risultati in Security Hub CSPM

AWSSecurity Hub CSPM dispone di funzionalità che modificano e agiscono automaticamente sui risultati in base alle specifiche dell'utente.

Security Hub CSPM attualmente supporta due tipi di automazioni:

- Regole di automazione: aggiorna e sopprime automaticamente i risultati quasi in tempo reale in base a criteri definiti dall'utente.
- Risposta e correzione automatizzate: crea EventBridge regole Amazon personalizzate che definiscono azioni automatiche da intraprendere in base a risultati e approfondimenti specifici.

Le regole di automazione sono utili quando desideri aggiornare automaticamente i campi di ricerca nel AWS Security Finding Format (ASFF). Ad esempio, puoi utilizzare una regola di automazione per aggiornare il livello di gravità o lo stato del flusso di lavoro dei risultati di specifiche integrazioni di terze parti. L'utilizzo della regola di automazione elimina la necessità di aggiornare manualmente il livello di gravità o lo stato del flusso di lavoro di ogni risultato di questo prodotto di terze parti.

EventBridge le regole sono utili quando si desidera intraprendere azioni al di fuori di Security Hub CSPM in relazione a risultati specifici o inviare risultati specifici a strumenti di terze parti per la correzione o ulteriori indagini. Le regole possono essere utilizzate per attivare azioni supportate, come richiamare una AWS Lambda funzione o notificare un argomento di Amazon Simple Notification Service (Amazon SNS) su un risultato specifico.

Le regole di automazione entrano in vigore prima dell' EventBridge applicazione delle regole. Cioè, le regole di automazione vengono attivate e aggiornano un risultato prima di EventBridge riceverlo. EventBridge le regole si applicano quindi al risultato aggiornato.

Quando configuri le automazioni per i controlli di sicurezza, consigliamo di filtrare in base all'ID del controllo anziché al titolo o alla descrizione. Mentre Security Hub CSPM aggiorna occasionalmente i titoli e le descrizioni dei controlli, gli ID di controllo rimangono invariati.

Argomenti

- Comprensione delle regole di automazione in Security Hub CSPM

- Utilizzo EventBridge per la risposta e la correzione automatiche

Comprensione delle regole di automazione in Security Hub CSPM

È possibile utilizzare le regole di automazione per aggiornare automaticamente i risultati in AWS Security Hub CSPM. Man mano che acquisisce i risultati, Security Hub CSPM può applicare una serie di azioni relative alle regole, come sopprimere i risultati, modificarne la gravità e aggiungere note. Tali azioni relative alle regole modificano i risultati che corrispondono ai criteri specificati.

Di seguito sono riportati alcuni esempi di casi d'uso per le regole di automazione:

- Elevare il livello di gravità di un risultato a `CRITICAL` se l'ID della risorsa del risultato si riferisce a una risorsa fondamentale per l'azienda.
- Elevare la gravità di un risultato `HIGH` da `CRITICAL` se il risultato influisce sulle risorse di specifici account di produzione.
- Assegnazione di risultati specifici che hanno la stessa gravità dello stato del `SUPPRESSED` flusso `INFORMATIONAL` di lavoro.

È possibile creare e gestire le regole di automazione solo da un account amministratore CSPM di Security Hub.

Le regole si applicano sia ai nuovi risultati che ai risultati aggiornati. È possibile creare una regola personalizzata da zero o utilizzare un modello di regola fornito da Security Hub CSPM. Puoi anche iniziare con un modello e modificarlo secondo necessità.

Definizione dei criteri e delle azioni delle regole

Da un account amministratore CSPM di Security Hub, è possibile creare una regola di automazione definendo uno o più criteri di regola e una o più azioni delle regole. Quando un risultato corrisponde ai criteri definiti, Security Hub CSPM applica le azioni della regola ad esso. Per ulteriori informazioni sui criteri e le azioni disponibili, vedere. Criteri e azioni delle regole disponibili

Security Hub CSPM attualmente supporta un massimo di 100 regole di automazione per ogni account amministratore.

L'account amministratore CSPM di Security Hub può anche modificare, visualizzare ed eliminare le regole di automazione. Una regola si applica ai risultati corrispondenti nell'account amministratore e in tutti i relativi account membri. Fornendo gli ID degli account dei membri come criteri di regola,

gli amministratori CSPM di Security Hub possono anche utilizzare le regole di automazione per aggiornare o eliminare i risultati in account membri specifici.

Una regola di automazione si applica solo nel luogo Regione AWS in cui è stata creata. Per applicare una regola in più regioni, l'amministratore deve creare la regola in ciascuna regione. Questa operazione può essere eseguita tramite la console CSPM di Security Hub, l'API CSPM di Security Hub o. AWS CloudFormation È inoltre possibile utilizzare uno script di distribuzione multiregionale.

Criteri e azioni delle regole disponibili

I seguenti campi ASFF (AWSSecurity Finding Format) sono attualmente supportati come criteri per le regole di automazione:

Criterio della regola	Operatori di filtro	Tipo di campo
`AwsAccountId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`AwsAccountName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`CompanyName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`ComplianceAssociatedStandardsId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`ComplianceSecurityControlId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa

Criterio della regola	Operatori di filtro	Tipo di campo
ComplianceStatus	Is, Is Not	Seleziona: [FAILED,,NOT_AVAILABLE ,PASSED] WARNING
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Numero
CreatedAt	Start, End, DateRange	Data (formattata come T21:47:39.269Z 2022-12-01)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Numero
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
FirstObservedAt	Start, End, DateRange	Data (formattata come 2022-12-01) T21:47:39.269Z
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa

Criterio della regola	Operatori di filtro	Tipo di campo
`LastObservedAt`	`Start, End, DateRange`	Data (formattata come 2022-12-01) T21:47:39.269Z
`NoteText`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`NoteUpdatedAt`	`Start, End, DateRange`	Data (formattata come 2022-12-01) T21:47:39.269Z
`NoteUpdatedBy`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`ProductArn`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`ProductName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`RecordState`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`RelatedFindingsId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa

Criterio della regola	Operatori di filtro	Tipo di campo
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Eseguire la mappatura
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa

Criterio della regola	Operatori di filtro	Tipo di campo
`ResourceTags`	`CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS`	Eseguire la mappatura
`ResourceType`	`Is, Is Not`	Seleziona (vedi Risorse supportate da ASFF)
`SeverityLabel`	`Is, Is Not`	Seleziona: [`CRITICAL,HIGH, MEDIUMLOW,INFORMATIONAL `]
`SourceUrl`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`Title`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`Type`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`UpdatedAt`	`Start, End, DateRange`	Data (formattata come T21:47:39.269Z 2022-12-01)
`UserDefinedFields`	`CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS`	Eseguire la mappatura

Criterio della regola	Operatori di filtro	Tipo di campo
`VerificationState`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Stringa
`WorkflowStatus`	`Is, Is Not`	Seleziona: [,,] `NEW` `NOTIFIED` `RESOLVED` `SUPPRESSED`

Per i criteri etichettati come campi stringa, l'utilizzo di operatori di filtro diversi sullo stesso campo influisce sulla logica di valutazione. Per ulteriori informazioni, consulta il riferimento StringFilterall'API CSPM AWS di Security Hub.

Ogni criterio supporta un numero massimo di valori che possono essere utilizzati per filtrare i risultati corrispondenti. Per i limiti di ogni criterio, vedere AutomationRulesFindingFiltersil riferimento all'API CSPM AWS di Security Hub.

I seguenti campi ASFF sono attualmente supportati come azioni per le regole di automazione:

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Per ulteriori informazioni su campi ASFF specifici, vedere la sintassi del AWSSecurity Finding Format (ASFF).

> **Tip**
>
> Se desideri che Security Hub CSPM smetta di generare risultati per un controllo specifico, ti consigliamo di disabilitare il controllo anziché utilizzare una regola di automazione. Quando disabiliti un controllo, Security Hub CSPM interrompe l'esecuzione dei controlli di sicurezza e la generazione dei relativi risultati, in modo da non incorrere in costi per tale controllo. Consigliamo di utilizzare le regole di automazione per modificare i valori di campi ASFF specifici per i risultati che soddisfano i criteri definiti. Per ulteriori informazioni sulla disabilitazione dei controlli, consulta. Disattivazione dei controlli in Security Hub CSPM

Risultati valutati dalle regole di automazione

Una regola di automazione valuta i risultati nuovi e aggiornati che Security Hub CSPM genera o inserisce tramite l'BatchImportFindingsoperazione dopo la creazione della regola. Security Hub CSPM aggiorna i risultati del controllo ogni 12-24 ore o quando la risorsa associata cambia stato. Per ulteriori informazioni, consulta Pianificazione dell'esecuzione dei controlli di sicurezza.

Le regole di automazione valutano i risultati originali forniti dal provider. I provider possono fornire nuovi risultati e aggiornare i risultati esistenti utilizzando il `BatchImportFindings` funzionamento dell'API CSPM Security Hub. Se i seguenti campi non esistono nel risultato originale, Security Hub CSPM popola automaticamente i campi e quindi utilizza i valori popolati nella valutazione mediante la regola di automazione:

- `AwsAccountName`
- `CompanyName`
- `ProductName`
- `Resource.Tags`
- `Workflow.Status`

Dopo aver creato una o più regole di automazione, le regole non vengono attivate se si aggiornano i campi di ricerca utilizzando l'operazione. BatchUpdateFindings Se crei una regola di automazione e apporti un `BatchUpdateFindings` aggiornamento che influiscono entrambi sullo stesso campo di ricerca, l'ultimo aggiornamento imposta il valore per quel campo. Prendiamo l'esempio seguente:

1. Si utilizza l'`BatchUpdateFindings`operazione per modificare il valore del `Workflow.Status` campo di un risultato da `NEW` a`NOTIFIED`.

2. Se chiamiGetFindings, il Workflow.Status campo ora ha un valore diNOTIFIED.
3. Si crea una regola di automazione che modifica il Workflow.Status campo del risultato da NEW aSUPPRESSED. (Ricorda che le regole ignorano gli aggiornamenti effettuati utilizzando l'BatchUpdateFindingsoperazione.)
4. Il fornitore dei risultati utilizza l'BatchImportFindingsoperazione per aggiornare il risultato e modifica il valore del Workflow.Status campo del risultato inNEW.
5. Se chiamiGetFindings, il Workflow.Status campo ora ha un valore diSUPPRESSED. Ciò è dovuto al fatto che è stata applicata la regola di automazione e la regola è stata l'ultima azione intrapresa sul risultato.

Quando si crea o si modifica una regola sulla console CSPM di Security Hub, la console visualizza una versione beta dei risultati che corrispondono ai criteri della regola. Mentre le regole di automazione valutano i risultati originali inviati dal provider dei risultati, la versione beta della console riflette i risultati nel loro stato finale così come sarebbero mostrati in risposta all'GetFindingsoperazione (ovvero dopo l'applicazione delle azioni delle regole o di altri aggiornamenti al risultato).

Come funziona l'ordine delle regole

Quando si creano regole di automazione, si assegna a ciascuna regola un ordine. Ciò determina l'ordine in cui Security Hub CSPM applica le regole di automazione e diventa importante quando più regole si riferiscono allo stesso campo di ricerca o ricerca.

Quando più azioni delle regole si riferiscono allo stesso campo di ricerca o ricerca, la regola con il valore numerico più alto per l'ordine delle regole si applica per ultima e ha l'effetto finale.

Quando si crea una regola nella console CSPM di Security Hub, Security Hub CSPM assegna automaticamente l'ordine delle regole in base all'ordine di creazione delle regole. La regola creata più di recente ha il valore numerico più basso per l'ordine delle regole e pertanto viene applicata per prima. Security Hub CSPM applica le regole successive in ordine crescente.

Quando si crea una regola tramite l'API CSPM di Security Hub oAWS CLI, Security Hub CSPM, applica per prima la regola con il valore numerico più basso. RuleOrder Quindi applica le regole successive in ordine crescente. Se più risultati sono ugualiRuleOrder, Security Hub CSPM applica prima una regola con un valore precedente per il UpdatedAt campo (ovvero, la regola che è stata modificata più di recente si applica per ultima).

È possibile modificare l'ordine delle regole in qualsiasi momento.

Esempio di ordine delle regole:

Regola A (l'ordine delle regole è**1**):

- Criteri della regola A
  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type` è `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` è `NEW`
  - `Workflow.Status` = `ACTIVE`
- Azioni della regola A
  - Aggiorna `Confidence` a `95`
  - Aggiorna `Severity` a `CRITICAL`

Regola B (l'ordine delle regole è**2**):

- Criteri della regola B
  - `AwsAccountId` = `123456789012`
- Azioni della regola B
  - Aggiorna `Severity` a `INFORMATIONAL`

Le azioni della Regola A si applicano innanzitutto ai risultati CSPM di Security Hub che soddisfano i criteri della Regola A. Successivamente, le azioni della Regola B si applicano ai risultati CSPM di Security Hub con l'ID account specificato. In questo esempio, poiché la regola B si applica per ultima, il valore finale dei `Severity` risultati derivanti dall'ID account specificato è. `INFORMATIONAL` In base all'azione della Regola A, il valore finale dei `Confidence` risultati corrispondenti è`95`.

Creazione di regole di automazione

È possibile utilizzare una regola di automazione per aggiornare automaticamente i risultati in AWS Security Hub CSPM. È possibile creare una regola di automazione personalizzata partendo da zero o, nella console CSPM di Security Hub, utilizzare un modello di regola precompilato. Per informazioni di base sul funzionamento delle regole di automazione, consulta. Comprensione delle regole di automazione in Security Hub CSPM

È possibile creare una sola regola di automazione alla volta. Per creare più regole di automazione, segui le procedure della console più volte oppure chiama l'API o il comando più volte con i parametri desiderati.

Devi creare una regola di automazione in ogni regione e account in cui desideri che la regola si applichi ai risultati.

Quando si crea una regola di automazione nella console CSPM di Security Hub, Security Hub CSPM mostra una versione beta dei risultati a cui si applica la regola. La versione beta non è attualmente supportata se i criteri della regola includono un filtro CONTAINS o NOT_CONTAINS. Puoi scegliere questi filtri per i tipi di campi di tipo map e string.

> **Important**
>
> AWSconsiglia di non includere informazioni di identificazione personale, riservate o sensibili nel nome della regola, nella descrizione o in altri campi.

Creazione di una regola di automazione personalizzata

Scegli il tuo metodo preferito e completa i passaggi seguenti per creare una regola di automazione personalizzata.

Console

Per creare una regola di automazione personalizzata (console)

1. Utilizzando le credenziali dell'amministratore CSPM di Security Hub, aprire la console CSPM di AWS Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Automazioni.
3. Scegli Crea regola. Per Tipo di regola, scegli Crea regola personalizzata.
4. Nella sezione Regola, fornisci un nome e una descrizione univoci per la regola.
5. Per Criteri, utilizza i menu a discesa Chiave, Operatore e Valore per specificare i criteri della regola. È necessario specificare almeno un criterio di regola.

   Se i criteri selezionati sono supportati, la console mostra una versione beta dei risultati che corrispondono ai criteri specificati.

6. Per l'azione automatizzata, utilizza i menu a discesa per specificare quali campi di ricerca aggiornare quando i risultati soddisfano i criteri delle regole. È necessario specificare almeno un'azione relativa alla regola.
7. Per lo stato della regola, scegli se desideri che la regola sia abilitata o disabilitata dopo la creazione.
8. (Facoltativo) Espandi la sezione Impostazioni aggiuntive. Seleziona Ignora le regole successive per i risultati che corrispondono a questi criteri se desideri che questa regola sia l'ultima regola applicata ai risultati che soddisfano i criteri della regola.
9. (Facoltativo) Per i tag, aggiungi i tag come coppie chiave-valore per aiutarti a identificare facilmente la regola.
10. Scegli Crea regola.

API

Per creare una regola di automazione (API) personalizzata

1. Esegui `CreateAutomationRule`dall'account amministratore CSPM di Security Hub. Questa API crea una regola con un Amazon Resource Name (ARN) specifico.
2. Fornisci un nome e una descrizione per la regola.
3. Imposta il `IsTerminal` parametro su `true` se desideri che questa regola sia l'ultima regola applicata ai risultati che soddisfano i criteri della regola.
4. Per il `RuleOrder` parametro, specificate l'ordine della regola. Security Hub CSPM applica prima le regole con un valore numerico inferiore per questo parametro.
5. Per il `RuleStatus` parametro, specificate se desiderate abilitare Security Hub CSPM e iniziate ad applicare la regola ai risultati dopo la creazione. Se non viene specificato alcun valore, il valore predefinito è `ENABLED`. Un valore di `DISABLED` indica che la regola viene messa in pausa dopo la creazione.
6. Per il `Criteria` parametro, fornite i criteri che desiderate che Security Hub CSPM utilizzi per filtrare i risultati. L'azione della regola si applicherà ai risultati che corrispondono ai criteri. Per un elenco dei criteri supportati, vedereCriteri e azioni delle regole disponibili.
7. Per il `Actions` parametro, specificate le azioni che desiderate che Security Hub CSPM intraprenda quando c'è una corrispondenza tra un risultato e i criteri definiti. Per un elenco delle azioni supportate, consulta. Criteri e azioni delle regole disponibili

Il AWS CLI comando di esempio seguente crea una regola di automazione che aggiorna lo stato del flusso di lavoro e la nota dei risultati corrispondenti. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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
```

Creazione di una regola di automazione da un modello (solo console)

I modelli di regole riflettono i casi d'uso comuni delle regole di automazione. Attualmente, solo la console CSPM di Security Hub supporta i modelli di regole. Completa i seguenti passaggi per creare una regola di automazione da un modello nella console.

Per creare una regola di automazione da un modello (console)

1. Utilizzando le credenziali dell'amministratore CSPM di Security Hub, aprire la console CSPM di AWS Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

2. Nel riquadro di navigazione, scegli Automazioni.
3. Scegli Crea regola. Per Tipo di regola, scegli Crea una regola dal modello.
4. Seleziona un modello di regola dal menu a discesa.
5. (Facoltativo) Se necessario per il tuo caso d'uso, modifica le sezioni Regola, Criteri e Azione automatizzata. È necessario specificare almeno un criterio di regola e un'azione della regola.

   Se i criteri selezionati sono supportati, la console mostra una versione beta dei risultati che corrispondono ai criteri specificati.
6. Per lo stato della regola, scegli se desideri che la regola sia abilitata o disabilitata dopo la creazione.
7. (Facoltativo) Espandi la sezione Impostazioni aggiuntive. Seleziona Ignora le regole successive per i risultati che corrispondono a questi criteri se desideri che questa regola sia l'ultima regola applicata ai risultati che soddisfano i criteri della regola.
8. (Facoltativo) Per i tag, aggiungi i tag come coppie chiave-valore per aiutarti a identificare facilmente la regola.
9. Scegli Crea regola.

Visualizzazione delle regole di automazione

È possibile utilizzare una regola di automazione per aggiornare automaticamente i risultati in AWS Security Hub CSPM. Per informazioni di base sul funzionamento delle regole di automazione, consulta. Comprensione delle regole di automazione in Security Hub CSPM

Scegli il tuo metodo preferito e segui i passaggi per visualizzare le regole di automazione esistenti e i dettagli di ciascuna regola.

Per visualizzare una cronologia di come le regole di automazione hanno modificato i risultati, consultaRevisione dei dettagli e della cronologia dei risultati in Security Hub CSPM.

Console

Per visualizzare le regole di automazione (console)

1. Utilizzando le credenziali dell'amministratore CSPM di Security Hub, aprire la console CSPM di AWS Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Automazioni.

3. Scegli il nome di una regola. In alternativa, seleziona una regola.
4. Scegli Azioni e Visualizza.

API

Per visualizzare le regole di automazione (API)

1. Per visualizzare le regole di automazione per il tuo account, esegui `ListAutomationRules`dall'account amministratore CSPM di Security Hub. Questa API restituisce gli ARN delle regole e altri metadati relativi alle regole. Non sono richiesti parametri di input per questa API, ma puoi opzionalmente fornire un limite `MaxResults` al numero di risultati e `NextToken` come parametro di paginazione. Il valore iniziale di `NextToken` dovrebbe essere. `NULL`
2. Per ulteriori dettagli sulla regola, inclusi i criteri e le azioni per una regola, esegui `BatchGetAutomationRules`dall'account amministratore CSPM di Security Hub. Fornisci gli ARN delle regole di automazione per le quali desideri i dettagli.

   L'esempio seguente recupera i dettagli per le regole di automazione specificate. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

   ```
   $ 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
   ```

Modifica delle regole di automazione

È possibile utilizzare una regola di automazione per aggiornare automaticamente i risultati in AWS Security Hub CSPM. Per informazioni di base sul funzionamento delle regole di automazione, consulta. Comprensione delle regole di automazione in Security Hub CSPM

Dopo aver creato una regola di automazione, l'amministratore CSPM di Security Hub delegato può modificare la regola. Quando si modifica una regola di automazione, le modifiche si applicano ai risultati nuovi e aggiornati che Security Hub CSPM genera o inserisce dopo la modifica della regola.

Scegli il metodo preferito e segui i passaggi per modificare il contenuto di una regola di automazione. Puoi modificare una o più regole con una sola richiesta. Per istruzioni sulla modifica dell'ordine delle regole, vedereModifica dell'ordine delle regole di automazione.

Console

Per modificare le regole di automazione (console)

1. Utilizzando le credenziali dell'amministratore CSPM di Security Hub, aprire la console CSPM di AWS Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Automazioni.
3. Seleziona la regola che desideri modificare. Scegli Azione e Modifica.
4. Modifica la regola come desideri e scegli Salva modifiche.

API

Per modificare le regole di automazione (API)

1. Esegui `BatchUpdateAutomationRules`dall'account amministratore CSPM di Security Hub.
2. Per il `RuleArn` parametro, fornite l'ARN delle regole che desiderate modificare.
3. Fornite i nuovi valori per i parametri che desiderate modificare. È possibile modificare qualsiasi parametro tranne`RuleArn`.

L'esempio seguente aggiornala regola di automazione specificata. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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
```

Modifica dell'ordine delle regole di automazione

È possibile utilizzare una regola di automazione per aggiornare automaticamente i risultati in AWS Security Hub CSPM. Per informazioni di base sul funzionamento delle regole di automazione, consulta. Comprensione delle regole di automazione in Security Hub CSPM

Dopo aver creato una regola di automazione, l'amministratore CSPM di Security Hub delegato può modificare la regola.

Se desideri mantenere invariati i criteri e le azioni della regola, ma modificare l'ordine in cui Security Hub CSPM applica una regola di automazione, puoi modificare solo l'ordine delle regole. Scegli il metodo preferito e segui i passaggi per modificare l'ordine delle regole.

Per istruzioni sulla modifica dei criteri o delle azioni di una regola di automazione, consultaModifica delle regole di automazione.

Console

Per modificare l'ordine delle regole di automazione (console)

1. Utilizzando le credenziali dell'amministratore CSPM di Security Hub, aprire la console CSPM di AWS Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/

2. Nel riquadro di navigazione, scegli Automazioni.
3. Seleziona la regola di cui desideri modificare l'ordine. Scegli Modifica priorità.
4. Scegli Sposta su per aumentare la priorità della regola di un'unità. Scegli Sposta giù per ridurre la priorità della regola di un'unità. Scegli Sposta in alto per assegnare alla regola un ordine pari a 1 (in questo modo la regola ha la precedenza sulle altre regole esistenti).

> **Note**
>
> Quando si crea una regola nella console CSPM di Security Hub, Security Hub CSPM assegna automaticamente l'ordine delle regole in base all'ordine di creazione delle regole. La regola creata più di recente ha il valore numerico più basso per l'ordine delle regole e pertanto viene applicata per prima.

API

Per modificare l'ordine delle regole di automazione (API)

1. Usa l'`BatchUpdateAutomationRules`operazione dall'account amministratore CSPM di Security Hub.
2. Per il `RuleArn` parametro, fornite l'ARN delle regole di cui desiderate modificare l'ordine.
3. Modifica il valore del `RuleOrder` campo.

> **Note**
>
> Se più regole hanno le stesse`RuleOrder`, Security Hub CSPM applica prima una regola con un valore precedente per il `UpdatedAt` campo (ovvero, la regola che è stata modificata più di recente si applica per ultima).

Eliminazione o disabilitazione delle regole di automazione

È possibile utilizzare una regola di automazione per aggiornare automaticamente i risultati in AWS Security Hub CSPM. Per informazioni di base sul funzionamento delle regole di automazione, consulta. Comprensione delle regole di automazione in Security Hub CSPM

Quando elimini una regola di automazione, Security Hub CSPM la rimuove dal tuo account e non applica più la regola ai risultati. In alternativa all'eliminazione, puoi disabilitare una regola. Ciò mantiene la regola per utilizzi futuri, ma Security Hub CSPM non applicherà la regola a nessun risultato corrispondente finché non lo abiliti.

Scegli il tuo metodo preferito e segui i passaggi per eliminare una regola di automazione. Puoi eliminare una o più regole in un'unica richiesta.

Console

Per eliminare o disabilitare le regole di automazione (console)

1. Utilizzando le credenziali dell'amministratore CSPM di Security Hub, aprire la console CSPM di AWS Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Automazioni.
3. Seleziona le regole che desideri eliminare. Scegliete Azione ed Elimina (per mantenere una regola, ma disattivarla temporaneamente, scegliete Disabilita).
4. Conferma la scelta e seleziona Delete (Elimina).

API

Per eliminare o disabilitare le regole di automazione (API)

1. Usa l'`BatchDeleteAutomationRules`operazione dall'account amministratore CSPM di Security Hub.
2. Per il `AutomationRulesArns` parametro, fornisci l'ARN delle regole che desideri eliminare (per mantenere una regola, ma disabilitarla temporaneamente, inserisci `DISABLED` il `RuleStatus` parametro).

L'esempio seguente elimina la regola di automazione specificata. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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
```

Esempi di regole di automazione

Questa sezione fornisce esempi di regole di automazione per i casi d'uso CSPM più comuni di Security Hub. Questi esempi corrispondono ai modelli di regole disponibili nella console CSPM di Security Hub.

Elevate la severità a Critica quando una risorsa specifica, come un bucket S3, è a rischio

In questo esempio, i criteri della regola vengono soddisfatti quando il `ResourceId` risultato è un bucket Amazon Simple Storage Service (Amazon S3) specifico. L'azione della regola consiste nel modificare la gravità dei risultati corrispondenti in. `CRITICAL` È possibile modificare questo modello per applicarlo ad altre risorse.

Esempio di richiesta API:

```
{
    "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"
            }
        }
    }]
}
```

Esempio di comando CLI:

```
$
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
```

Elevare la severità dei risultati relativi alle risorse negli account di produzione

In questo esempio, i criteri della regola vengono soddisfatti quando viene generato un risultato di `HIGH` gravità in conti di produzione specifici. L'azione della regola consiste nel modificare la gravità dei risultati corrispondenti in. `CRITICAL`

Esempio di richiesta API:

```
{
    "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"
            }
        }
    }]
}
```

Esempio di comando CLI:

```
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
```

Sopprime i risultati informativi

In questo esempio, i criteri della regola vengono soddisfatti per i risultati di `INFORMATIONAL` gravità inviati a Security Hub CSPM da Amazon. GuardDuty L'azione della regola consiste nel modificare lo stato del flusso di lavoro dei risultati corrispondenti in. `SUPPRESSED`

Esempio di richiesta API:

```
{
    "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"
            }
        }
    }]
}
```

Esempio di comando CLI:

```
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
```

Utilizzo EventBridge per la risposta e la correzione automatiche

Creando regole in Amazon EventBridge, puoi rispondere automaticamente ai risultati del CSPM di AWS Security Hub. Security Hub CSPM invia i risultati come eventi in tempo quasi reale. EventBridge Puoi scrivere regole semplici per indicare a quali eventi sei interessato e quali azioni automatiche intraprendere quando un evento corrisponde a una regola. Le azioni che possono essere attivate automaticamente includono le seguenti:

- Richiamare una funzione AWS Lambda
- Richiamo del comando run di Amazon EC2
- Inoltro dell'evento a Amazon Kinesis Data Streams
- Attivazione di una macchina a stati AWS Step Functions
- Notifica di un argomento Amazon SNS o di una coda Amazon SQS
- Invio di una ricerca a uno strumento di gestione di ticket, chat, SIEM o risposta agli incidenti di terze parti

Security Hub CSPM invia automaticamente tutti i nuovi risultati e tutti gli aggiornamenti ai EventBridge risultati esistenti come eventi. EventBridge Puoi anche creare azioni personalizzate che ti consentano di inviare risultati e approfondimenti selezionati a. EventBridge

Quindi configuri EventBridge le regole per rispondere a ciascun tipo di evento.

Per ulteriori informazioni sull'utilizzo EventBridge, consulta la Amazon EventBridge User Guide .

> **Note**
>
> Come best practice, assicurati che le autorizzazioni concesse agli utenti per l'accesso EventBridge utilizzino politiche IAM AWS Identity and Access Management (Least-Privilege) che concedano solo le autorizzazioni richieste.

Per ulteriori informazioni, consulta Gestione delle identità e degli accessi in Amazon. EventBridge

In Solutions è disponibile anche una serie di modelli per la risposta e la correzione automatiche tra più account. AWS I modelli sfruttano le regole EventBridge degli eventi e le funzioni Lambda. Distribuisci la soluzione utilizzando e. CloudFormation AWS Systems Manager La soluzione può creare azioni di risposta e riparazione completamente automatiche. Può anche utilizzare azioni personalizzate Security Hub CSPM per creare azioni di risposta e correzione attivate dall'utente. Per i dettagli su come configurare e utilizzare la soluzione, consulta la pagina Automated Security Response on solution. AWS

Argomenti

- Tipi di eventi CSPM di Security Hub in EventBridge
- EventBridge formati di eventi per Security Hub CSPM
- Configurazione di una EventBridge regola per i risultati del CSPM di Security Hub
- Utilizzo di azioni personalizzate per inviare risultati e approfondimenti a EventBridge

Tipi di eventi CSPM di Security Hub in EventBridge

Security Hub CSPM utilizza i seguenti tipi di EventBridge eventi Amazon per l'integrazione con. EventBridge

Nella EventBridge dashboard di Security Hub CSPM, All Events include tutti questi tipi di eventi.

Tutti i risultati (Risultati del Security Hub - Importati)

Security Hub CSPM invia automaticamente tutti i nuovi risultati e tutti gli aggiornamenti ai risultati esistenti EventBridge come Security Hub Findings - Imported eventi. Ogni Security Hub Findings - Imported evento contiene un singolo risultato.

Ogni `BatchImportFindings` `BatchUpdateFindings` richiesta innesca un Security Hub Findings - Imported evento.

Per gli account amministratore, il feed degli eventi EventBridge include eventi relativi ai risultati relativi all'account e agli account dei membri.

In una regione di aggregazione, il feed degli eventi include gli eventi relativi ai risultati della regione di aggregazione e delle regioni collegate. Cross-Region i risultati sono inclusi nel feed degli eventi quasi

in tempo reale. Per informazioni su come configurare l'aggregazione dei risultati, vederethe section called "Aggregazione dei dati tra le regioni".

È possibile definire regole EventBridge che indirizzino automaticamente i risultati a un flusso di lavoro di correzione, a uno strumento di terze parti o a un altro obiettivo supportato EventBridge . Le regole possono includere filtri che applicano la regola solo se il risultato ha valori di attributo specifici.

Si utilizza questo metodo per inviare automaticamente tutti i risultati, o tutti i risultati con caratteristiche specifiche, a un flusso di lavoro di risposta o correzione.

Per informazioni, consulta the section called "Configurazione di una regola EventBridge ".

Risultati per azioni personalizzate (Risultati di Security Hub - Azione personalizzata)

Security Hub CSPM invia anche i risultati associati alle azioni personalizzate EventBridge come Security Hub Findings - Custom Action eventi.

Ciò è utile per gli analisti che utilizzano la console Security Hub CSPM e desiderano inviare un risultato specifico, o un piccolo insieme di risultati, a un flusso di lavoro di risposta o correzione. È possibile selezionare un'operazione personalizzata per un massimo di 20 risultati alla volta. Ogni risultato viene inviato EventBridge come evento separato. EventBridge

Quando crei un'azione personalizzata, le assegni un ID di azione personalizzato. È possibile utilizzare questo ID per creare una EventBridge regola che esegue un'azione specificata dopo aver ricevuto un risultato associato a tale ID di azione personalizzato.

Per informazioni, consulta the section called "Configurazione e utilizzo di azioni personalizzate".

Ad esempio, è possibile creare un'azione personalizzata in Security Hub chiamata CSPM. `send_to_ticketing` Quindi EventBridge, si crea una regola che viene attivata quando si EventBridge riceve un risultato che include l'ID dell'azione `send_to_ticketing` personalizzato. La regola include la logica per inviare il risultato al sistema di ticket. È quindi possibile selezionare i risultati all'interno di Security Hub CSPM e utilizzare l'azione personalizzata in Security Hub CSPM per inviare manualmente i risultati al sistema di ticketing.

Per esempi su come inviare i risultati del CSPM di Security Hub EventBridge per un'ulteriore elaborazione, consulta Come integrare le azioni personalizzate di AWS Security Hub CSPM con PagerDuty e Come abilitare le azioni personalizzate in Security Hub CSPM sul blog Partner Network (AWS APN). AWS

Risultati di approfondimento per azioni personalizzate (Risultati di Security Hub Insight)

Puoi anche utilizzare azioni personalizzate per inviare set di risultati di insight EventBridge come Security Hub Insight Results eventi. I risultati di Insight sono le risorse che corrispondono a un insight. Tieni presente che quando invii i risultati degli approfondimenti a EventBridge, non stai inviando i risultati a EventBridge. Stai inviando solo gli identificatori delle risorse associati ai risultati degli approfondimenti. È possibile inviare fino a 100 identificatori di risorse alla volta.

Analogamente alle azioni personalizzate per i risultati, si crea prima l'azione personalizzata in Security Hub CSPM, quindi si crea una regola in. EventBridge

Per informazioni, consulta the section called "Configurazione e utilizzo di azioni personalizzate".

Ad esempio, supponiamo di vedere un particolare risultato di interesse che desideri condividere con un collega. In tal caso, puoi utilizzare un'azione personalizzata per inviare il risultato dell'approfondimento al collega tramite una chat o un sistema di ticket.

EventBridge formati di eventi per Security Hub CSPM

I tipi di Security Hub Insight Results evento Security Hub Findings - Imported Security Findings - Custom Action, e utilizzano i seguenti formati di evento.

Il formato dell'evento è il formato utilizzato quando Security Hub CSPM invia un evento a. EventBridge

Risultati di Security Hub - Importati

Security Hub Findings - Importedeventi inviati da Security Hub CSPM EventBridge utilizzando il seguente formato.

```
{
   "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>*è il contenuto, in formato JSON, del risultato inviato dall'evento. Ogni evento invia un singolo risultato.

Per un elenco completo degli attributi di ricerca, vedereAWS Formato ASFF (Security Finding Format).

Per informazioni su come configurare EventBridge le regole che vengono attivate da questi eventi, vederethe section called "Configurazione di una regola EventBridge ".

Risultati di Security Hub - Azione personalizzata

Security Hub Findings - Custom Actioneventi inviati da Security Hub CSPM EventBridge utilizzando il seguente formato. Ogni risultato viene inviato in un evento separato.

```
{
  "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>*è il contenuto, in formato JSON, del risultato inviato dall'evento. Ogni evento invia un singolo risultato.

Per un elenco completo degli attributi di ricerca, vedereAWS Formato ASFF (Security Finding Format).

Per informazioni su come configurare EventBridge le regole che vengono attivate da questi eventi, vederethe section called "Configurazione e utilizzo di azioni personalizzate".

Risultati di Security Hub Insight

Security Hub Insight Resultseventi inviati da Security Hub CSPM per EventBridge utilizzare il seguente formato.

```
{
  "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}
    ]
  }
}
```

Per informazioni su come creare una EventBridge regola che viene attivata da questi eventi, vedere. the section called "Configurazione e utilizzo di azioni personalizzate"

Configurazione di una EventBridge regola per i risultati del CSPM di Security Hub

Puoi creare una regola in Amazon EventBridge che definisce un'azione da intraprendere quando viene ricevuto un Security Hub Findings - Imported evento. Security Hub Findings - Importedgli eventi vengono attivati dagli aggiornamenti `BatchUpdateFindings` delle operazioni `BatchImportFindings` e delle operazioni.

Ogni regola contiene uno schema di eventi, che identifica gli eventi che attivano la regola. Il modello di evento contiene sempre l'origine dell'evento (`aws.securityhub`) e il tipo di evento (Security Hub Findings - Imported). Il pattern di eventi può anche specificare filtri per identificare i risultati a cui si applica la regola.

La regola dell'evento identifica quindi gli obiettivi della regola. Gli obiettivi sono le azioni da intraprendere quando si EventBridge riceve un evento Security Hub Findings - Imported e il risultato corrisponde ai filtri.

Le istruzioni fornite qui utilizzano la EventBridge console. Quando usi la console, crea EventBridge automaticamente la policy richiesta basata sulle risorse che consente di EventBridge scrivere su Amazon Logs. CloudWatch

Puoi anche utilizzare il `PutRule` funzionamento dell'API. EventBridge Tuttavia, se si utilizza l' EventBridge API, è necessario creare la policy basata sulle risorse. Per informazioni sulla policy richiesta, consulta le autorizzazioni CloudWatch dei log nella Amazon User Guide. EventBridge

Formato del modello di evento

Il formato del modello di evento per Security Hub Findings - Imported events è il seguente:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`identifica Security Hub CSPM come servizio che genera l'evento.
- `detail-type`identifica il tipo di evento.
- `detail`è opzionale e fornisce i valori di filtro per il pattern di eventi. Se il modello di evento non contiene un `detail` campo, tutti i risultati attivano la regola.

Puoi filtrare i risultati in base a qualsiasi attributo di ricerca. Per ogni attributo, fornisci una matrice separata da virgole di uno o più valori.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Se fornisci più di un valore per un attributo, questi valori vengono uniti da. `OR` Un risultato corrisponde al filtro per un singolo attributo se il risultato contiene uno dei valori elencati. Ad esempio, se fornisci entrambi i valori `INFORMATIONAL` e `LOW` come valori per`Severity.Label`, il risultato corrisponde se ha un'etichetta di gravità pari a uno `INFORMATIONAL` o`LOW`.

Gli attributi sono uniti da`AND`. Un risultato corrisponde se corrisponde ai criteri di filtro per tutti gli attributi forniti.

Quando si fornisce un valore di attributo, questo deve riflettere la posizione di tale attributo all'interno della struttura ASFF (AWS Security Finding Format).

> **Tip**
>
> Quando si filtrano i risultati dei controlli, si consiglia di utilizzare i campi `SecurityControlId` o `SecurityControlArn` ASFF come filtri, anziché o. `Title` `Description` Questi ultimi campi possono cambiare occasionalmente, mentre l'ID di controllo e l'ARN sono identificatori statici.

Nell'esempio seguente, il modello di evento fornisce valori di filtro per `ProductArn` e`Severity.Label`, pertanto, un risultato corrisponde se è generato da Amazon Inspector e ha un'etichetta di gravità pari a o. `INFORMATIONAL` `LOW`

```
{
    "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"]
            }
        }
    }
}
```

Creazione di una regola di evento

È possibile utilizzare un modello di evento predefinito o un modello di evento personalizzato per creare una regola in EventBridge. Se si seleziona un modello predefinito, compila EventBridge automaticamente e. `source` `detail-type` EventBridge fornisce anche campi per specificare i valori di filtro per i seguenti attributi di ricerca:

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Per creare una EventBridge regola (console)

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Utilizzando i seguenti valori, crea una EventBridge regola che monitora la ricerca degli eventi:
    - Per Tipo di regola, scegli Regola con un modello di eventi.
    - Scegli come creare lo schema degli eventi.

Per creare il modello dell'evento con...	Esegui questa operazione…	
Un modello	Nella sezione Schema degli eventi, scegli le seguenti opzioni: • Per Origine evento, scegli Servizi AWS . • Per l'AWS assistenza, scegli Security Hub. • Per il tipo di evento, scegli Security Hub Findings - Imported. • (Facoltativo) Per rendere la regola più specifica, aggiungi i valori del filtro. Ad esempio, per limitare la regola ai risultati con stati di record attivi, per gli stati di record specifici, scegli Attivo.	

Per creare il modello dell'evento con...	Esegui questa operazione…
Un modello di evento personalizzato (Utilizza uno schema personalizzato se desideri filtrare i risultati in base agli attributi che non vengono visualizzati nella EventBridge console.)	• Nella sezione Schema di eventi, scegli Modelli personalizzati (editor JSON), quindi incolla il seguente modello di evento nell'area di testo: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>" ] } } }` • Aggiorna il modello di evento per includere l'attributo e i valori degli attributi che desideri utilizzare come filtro. Ad esempio, per applicare la regola ai risultati che hanno uno stato di verifica di `TRUE_POSITIVE` ,

Per creare il modello dell'evento con...	Esegui questa operazione…	
	utilizza il seguente esempio di modello: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } } }`	

- Per i tipi di target, scegli il AWS servizio e per Seleziona un target, scegli un obiettivo, ad esempio un argomento o una AWS Lambda funzione di Amazon SNS. La destinazione viene attivata quando viene ricevuto un evento che corrisponde al modello di evento definito nella regola.

Per informazioni dettagliate sulla creazione di regole, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi nella Amazon EventBridge User Guide.

Utilizzo di azioni personalizzate per inviare risultati e approfondimenti a EventBridge

Per utilizzare le azioni personalizzate AWS di Security Hub CSPM per inviare risultati o approfondimenti ad Amazon EventBridge, devi prima creare l'azione personalizzata in Security Hub CSPM. Quindi, puoi definire regole EventBridge che si applicano alle tue azioni personalizzate.

Puoi creare fino a 50 azioni personalizzate.

Se abiliti l'aggregazione tra regioni e gestisci i risultati dalla regione di aggregazione, crea azioni personalizzate nella regione di aggregazione.

La regola in EventBridge utilizza l'Amazon Resource Name (ARN) dell'azione personalizzata.

Creazione di un'azione personalizzata

Quando si crea un'azione personalizzata in AWS Security Hub CSPM, se ne specificano il nome, la descrizione e un identificatore univoco.

Un'azione personalizzata specifica quali azioni intraprendere quando un EventBridge evento corrisponde a una regola. EventBridge Security Hub CSPM invia ogni risultato EventBridge come evento.

Scegli il tuo metodo preferito e segui i passaggi per creare un'azione personalizzata.

Console

Per creare un'azione personalizzata in Security Hub CSPM (console)

1. Aprire la console AWS Security Hub CSPM all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegliere Settings (Impostazioni), quindi Custom actions (Operazioni personalizzate).
3. Scegliere Create custom action (Crea operazione personalizzata).
4. Fornire Name (Nome), Description (Descrizione) e Custom action ID (ID operazione personalizzata) per l'operazione.

   Il campo Name (Nome) non deve contenere più di 20 caratteri.

   L'ID dell'azione personalizzata deve essere univoco per ogni AWS account.
5. Scegliere Create custom action (Crea operazione personalizzata).
6. Prendere nota dell'operazione ARN personalizzata. È necessario utilizzare l'ARN quando si crea una regola da associare a questa operazione in EventBridge.

API

Per creare un'azione personalizzata (API)

Usa l'CreateActionTargetoperazione. Se stai usando il AWS CLI, esegui il comando create-action-target.

L'esempio seguente crea un'azione personalizzata per inviare i risultati a uno strumento di correzione. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

Definizione di una regola in EventBridge

Per attivare un'azione personalizzata in Amazon EventBridge, devi creare una regola corrispondente in. EventBridge La definizione della regola include l'Amazon Resource Name (ARN) dell'azione personalizzata.

Il modello di evento per un evento Security Hub Findings - Custom Action ha il seguente formato:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Il modello di evento per un evento Security Hub Insight Results ha il seguente formato:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

In entrambi i modelli, *<custom action ARN>* è l'ARN di un'azione personalizzata. È possibile configurare una regola che si applica a più di un'azione personalizzata.

Le istruzioni fornite qui si riferiscono alla EventBridge console. Quando si utilizza la console, crea EventBridge automaticamente la policy necessaria basata sulle risorse che consente di EventBridge scrivere su Logs. CloudWatch

Puoi anche utilizzare il funzionamento `PutRule` API dell'API. EventBridge Tuttavia, se si utilizza l' EventBridge API, è necessario creare la policy basata sulle risorse. Per i dettagli sulla policy richiesta, consulta le autorizzazioni CloudWatch dei log nella Amazon User Guide. EventBridge

Per definire una regola in EventBridge (EventBridge console)

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Crea regola.
4. Inserisci un nome e una descrizione per la regola.
5. Per Router di eventi, scegli quello che desideri associare a questa regola. Se vuoi che questa regola corrisponda agli eventi provenienti dal tuo account, seleziona Predefinito. Quando un servizio di AWS nell'account emette un evento, passa sempre al bus di eventi predefinito dell'account.
6. Per Tipo di regola, scegli Regola con un modello di eventi.
7. Scegli Next (Successivo).
8. Per Event source (Origine eventi), seleziona AWS events (Eventi).
9. Per Modello di eventi, scegli Modulo di modello di eventi.
10. Per Origine evento, scegli Servizi AWS .
11. Per l'AWS assistenza, scegli Security Hub.
12. Per Tipo di evento, procedere in uno dei seguenti modi:
    - Per creare una regola da applicare quando invii i risultati a un'azione personalizzata, scegli Security Hub Findings - Azione personalizzata.
    - Per creare una regola da applicare quando invii i risultati di Insight a un'azione personalizzata, scegli Security Hub Insight Results.
13. Scegli ARN per azioni personalizzate specifiche, aggiungi un ARN per azioni personalizzate.

Se la regola si applica a più azioni personalizzate, scegli Aggiungi per aggiungere altri ARN di azioni personalizzate.

14. Scegli Next (Successivo).
15. In Seleziona obiettivi, scegli e configura il target da richiamare quando questa regola viene soddisfatta.
16. Scegli Next (Successivo).
17. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta i EventBridge tag Amazon nella Amazon EventBridge User Guide.
18. Scegli Next (Successivo).
19. Rivedi i dettagli della regola e scegli Crea regola.

    Quando esegui un'azione personalizzata sui risultati o sugli insight del tuo account, vengono generati degli eventi in EventBridge.

Selezione di un'azione personalizzata per risultati e approfondimenti

Dopo aver creato le azioni personalizzate CSPM di AWS Security Hub e le EventBridge regole Amazon, puoi inviare risultati e approfondimenti a EventBridge per la gestione e l'elaborazione automatiche.

Gli eventi vengono inviati EventBridge solo nell'account in cui sono visualizzati. Se visualizzi un risultato utilizzando un account amministratore, l'evento viene inviato EventBridge all'account amministratore.

AWS Affinché le chiamate API siano efficaci, le implementazioni del codice di destinazione devono trasferire i ruoli negli account dei membri. Ciò significa anche che il ruolo a cui si passa deve essere distribuito a ciascun membro laddove è necessaria un'azione.

Per inviare i risultati a EventBridge (console)

1. Aprire la console AWS Security Hub CSPM all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Visualizza un elenco di risultati:

   - Da Findings, puoi visualizzare i risultati di tutte le integrazioni e i controlli di prodotto abilitati.

- Dagli standard di sicurezza, puoi accedere a un elenco di risultati generati da un controllo specifico. Per ulteriori informazioni, consulta Revisione dei dettagli dei controlli in Security Hub CSPM.
- Da Integrazioni, puoi accedere a un elenco di risultati generati da un'integrazione abilitata. Per ulteriori informazioni, consulta Visualizzazione dei risultati di un'integrazione CSPM di Security Hub.
- Da Insights, puoi accedere a un elenco di risultati per ottenere un risultato approfondito. Per ulteriori informazioni, consulta Revisione e azione in base agli approfondimenti in Security Hub CSPM.

3. Seleziona i risultati a cui inviare EventBridge. È possibile selezionare fino a 20 risultati alla volta.
4. In Azioni, scegli l'azione personalizzata che si allinea alla EventBridge regola da applicare.

   Security Hub CSPM invia un evento Security Hub Findings - Custom Action separato per ogni risultato.

Per inviare i risultati delle informazioni a EventBridge (console)

1. Aprire la console AWS Security Hub CSPM all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, seleziona Informazioni dettagliate.
3. Nella pagina Insights, scegli l'approfondimento che include i risultati a cui inviare. EventBridge
4. Seleziona i risultati degli approfondimenti a cui inviare EventBridge. Puoi selezionare fino a 20 risultati alla volta.
5. In Azioni, scegli l'azione personalizzata che si allinea alla EventBridge regola da applicare.

Utilizzo della dashboard in Security Hub CSPM

Sulla console Security Hub CSPM, la dashboard di riepilogo mostra un riepilogo dei rischi, delle sequenze di attacco e della copertura di sicurezza. Questa dashboard consente di identificare i rischi e le sequenze di attacco in base alla gravità e alla copertura dell'account per diverse funzionalità di sicurezza. Ogni volta che apri la dashboard, questa si aggiorna automaticamente. Tieni presente, tuttavia, che i punteggi di sicurezza e gli stati di controllo si aggiornano ogni 24 ore.

Puoi personalizzare la dashboard di riepilogo aggiungendo e rimuovendo diversi widget di sicurezza da essa. Puoi anche specificare criteri di filtro per recuperare e visualizzare particolari tipi di dati. Se

personalizzi la dashboard, Security Hub salva le impostazioni di personalizzazione. Se altri utenti del tuo account personalizzano la dashboard, le loro modifiche vengono salvate indipendentemente dalle tue impostazioni di personalizzazione.

Se hai configurato l'aggregazione tra regioni in Security Hub CSPM, la dashboard di riepilogo mostra i dati aggregati. Se il tuo account è l'account amministratore delegato di un'organizzazione, i dati includono i risultati relativi al tuo account e agli account dei membri. Se il tuo account è un account membro o un account autonomo, i dati includono i risultati solo per il tuo account.

Argomenti

- Widget disponibili per la dashboard di riepilogo
- Filtraggio della dashboard di riepilogo in Security Hub CSPM
- Personalizzazione della dashboard di riepilogo in Security Hub CSPM

Widget disponibili per la dashboard di riepilogo

La dashboard di riepilogo include widget che riflettono il moderno panorama delle minacce alla sicurezza del cloud, guidati dalle operazioni e dalle esperienze di sicurezza dei AWS clienti. Alcuni widget vengono visualizzati per impostazione predefinita, mentre altri no. Puoi personalizzare la visualizzazione della dashboard aggiungendo o rimuovendo widget.

Per aggiungere un widget, scegli Aggiungi widget nella parte superiore della dashboard. Puoi quindi sfogliare l'elenco dei widget disponibili o inserire il titolo di un widget nella barra di ricerca. Quando trovi il widget da aggiungere, trascinalo nella posizione in cui desideri che appaia sulla dashboard. Per ulteriori informazioni, consulta Personalizzazione della dashboard.

I widget sono mostrati per impostazione predefinita

Per impostazione predefinita, la dashboard Riepilogo include i seguenti widget.

Le principali sequenze di minacce

Visualizza le sequenze di minacce con la massima gravità. I risultati della sequenza delle minacce, noti come risultati delle sequenze di attacco in Amazon GuardDuty, mettono in correlazione più eventi per identificare potenziali minacce al tuo AWS ambiente. Le sequenze di minacce possono includere comportamenti di attacco in corso o recenti (entro una finestra temporale di 24 ore) nel tuo ambiente, che a loro volta possono portare a ulteriori compromessi.

È necessario che GuardDuty GuardDuty S3 Protection sia abilitato per ricevere i risultati della sequenza delle minacce in Security Hub CSPM.

Rischi principali

Visualizza un riepilogo dei principali rischi nell'ambiente in uso. La parte superiore del widget mostra il conteggio dei rischi per ogni livello di gravità. È possibile scegliere un livello di gravità per accedere alla pagina Rischi, con i rischi filtrati in base al livello di gravità selezionato. I rischi che presentano il maggior numero di ricorrenze nell'ambiente vengono visualizzati per primi. Questo widget consente di stabilire le priorità dei rischi da mitigare.

Copertura di sicurezza

Riassume l'estensione della copertura di sicurezza, in base ai risultati del controllo della copertura. I controlli di copertura verificano se una specifica funzionalità Servizio AWS e le relative funzionalità sono abilitate (ad esempio,[Macie.1] Amazon Macie dovrebbe essere abilitato). Questo widget ti aiuta ad assicurarti di disporre di `PASSED` risultati per il controllo della copertura. La console CSPM di Security Hub fornisce collegamenti da questo widget per aiutarti ad abilitare le funzionalità di sicurezza mancanti. Ti consigliamo di utilizzare la configurazione centrale per abilitare le funzionalità di sicurezza mancanti su più Account AWS e. Regioni AWS Per ulteriori informazioni, consulta Comprendere la configurazione centrale in Security Hub CSPM.

Standard di sicurezza

Visualizza il punteggio di sicurezza riepilogativo più recente e il punteggio di sicurezza per ogni standard CSPM di Security Hub. I punteggi di sicurezza, che vanno dallo 0 al 100 percento, rappresentano la percentuale di controlli superati rispetto a tutti i controlli abilitati. Per ulteriori informazioni su questi punteggi, vedere. Metodo di calcolo dei punteggi di sicurezza Questo widget ti aiuta a comprendere la tua posizione generale in materia di sicurezza.

Risorse con il maggior numero di risultati

Fornisce una panoramica delle risorse, degli account e delle applicazioni con il maggior numero di risultati. L'elenco è ordinato in ordine decrescente in base al numero di risultati. Nel widget, ogni scheda mostra i primi sei elementi di quella categoria, raggruppati per gravità e tipo di risorsa. Se scegli un numero nella colonna Risultati totali, Security Hub CSPM apre una pagina che mostra i risultati per l'asset. Questo widget ti aiuta a identificare rapidamente quali delle tue risorse principali presentano potenziali minacce alla sicurezza.

Risultati per regione

Mostra il numero totale di risultati, raggruppati per gravità, Regione AWS in ognuno dei quali è abilitato Security Hub CSPM. Questo widget consente di identificare i problemi di sicurezza

che potenzialmente interessano regioni particolari. Se apri la dashboard nella tua regione di aggregazione, questo widget ti aiuta a monitorare potenziali problemi di sicurezza in ogni regione collegata.

I tipi di minacce più comuni

Fornisce un'analisi dettagliata dei 10 tipi di minacce più comuni nell' AWS ambiente in uso. Ciò include minacce come l'aumento dei privilegi, l'uso di credenziali esposte o la comunicazione con indirizzi IP dannosi.

Per visualizzare questi dati, Amazon GuardDuty deve essere abilitato. In caso affermativo, scegli un tipo di minaccia in questo widget per aprire la GuardDuty console ed esaminare i risultati relativi a questa minaccia. Questo widget consente di valutare le potenziali minacce nel contesto di altri problemi di sicurezza.

Vulnerabilità del software con exploit

Fornisce un riepilogo delle vulnerabilità software presenti nell' AWS ambiente in uso e che presentano exploit noti. Puoi anche esaminare un'analisi dettagliata delle vulnerabilità per cui sono disponibili e non sono disponibili correzioni.

Per visualizzare questi dati, è necessario abilitare Amazon Inspector. In tal caso, scegli una statistica in questo widget per aprire la console Amazon Inspector e visualizzare ulteriori dettagli sulla vulnerabilità. Questo widget ti aiuta a valutare le vulnerabilità del software nel contesto di altri problemi di sicurezza.

Nuove scoperte nel tempo

Mostra l'andamento del numero di nuovi risultati giornalieri negli ultimi 90 giorni. Puoi suddividere i dati per gravità o per fornitore per un contesto aggiuntivo. Questo widget ti aiuta a capire se il volume di ricerca è aumentato o diminuito in momenti specifici negli ultimi 90 giorni.

Risorse con il maggior numero di risultati

Fornisce un riepilogo delle risorse che hanno generato il maggior numero di risultati, suddivise per i seguenti tipi di risorse: bucket Amazon Simple Storage Service (Amazon S3), istanze Amazon Elastic Compute Cloud (Amazon EC2) e funzioni. AWS Lambda

Nel widget, ogni scheda si concentra su uno dei tipi di risorse precedenti, elencando le 10 istanze di risorse che hanno generato il maggior numero di risultati. Per esaminare i risultati di una risorsa specifica, scegli l'istanza della risorsa. Questo widget ti aiuta a valutare i risultati di sicurezza associati a AWS risorse comuni.

Widget nascosti per impostazione predefinita

I seguenti widget sono disponibili anche per la dashboard Riepilogo, ma sono nascosti per impostazione predefinita.

AMI con il maggior numero di risultati

Fornisce un elenco delle 10 Amazon Machine Images (AMI) che hanno generato il maggior numero di risultati. Questi dati sono disponibili solo se Amazon EC2 è abilitato per il tuo account. Ti aiuta a identificare quali AMI rappresentano potenziali rischi per la sicurezza.

Principali IAM con il maggior numero di risultati

Fornisce un elenco dei 10 utenti AWS Identity and Access Management (IAM) che hanno generato il maggior numero di risultati. Questo widget consente di eseguire attività amministrative e di fatturazione. Mostra quali utenti contribuiscono maggiormente all'utilizzo del CSPM di Security Hub.

Account con il maggior numero di risultati (per gravità)

Mostra un grafico dei 10 account che hanno generato il maggior numero di risultati, raggruppati per gravità. Questo widget ti aiuta a determinare su quali account concentrare le attività di analisi e correzione.

Account con il maggior numero di risultati (per tipo di risorsa)

Mostra un grafico dei 10 account che hanno generato il maggior numero di risultati, raggruppati per tipo di risorsa. Questo widget consente di determinare a quali account e tipi di risorse dare priorità per l'analisi e la correzione.

Approfondimenti

Elenca cinque approfondimenti gestiti da Security Hub CSPM e il numero di risultati che hanno generato. Insights identifica un'area di sicurezza specifica che richiede attenzione.

I risultati più recenti delle AWS integrazioni

Mostra il numero di risultati ricevuti in Security Hub CSPM da integrated. Servizi AWS Mostra anche quando sono stati ricevuti più di recente i risultati di ciascun servizio integrato. Questo widget fornisce dati consolidati sui risultati provenienti da più Servizi AWS fonti. Per approfondire, scegli un servizio integrato. Security Hub CSPM apre quindi la console per quel servizio.

Filtraggio della dashboard di riepilogo in Security Hub CSPM

Puoi curare la dashboard di riepilogo sulla console CSPM di Security Hub in modo che includa solo i dati di sicurezza più pertinenti per te. Ad esempio, se fai parte di un team applicativo, potresti creare una visualizzazione dedicata per un'applicazione critica nel tuo ambiente di produzione. Se fai parte di un team di sicurezza, potresti creare una visualizzazione dedicata che ti aiuti a concentrarti sui risultati ad alta gravità.

Per creare queste visualizzazioni curate, inserisci i criteri di filtro nella casella del filtro sopra la dashboard. Se applichi criteri di filtro, i criteri si applicano a tutti i dati e i widget della dashboard, ad eccezione dei dati nei widget Insights and Security standards. Per un elenco dei widget disponibili nella dashboard, consulta. Widget disponibili per la dashboard di riepilogo

Puoi filtrare i dati utilizzando i seguenti campi:

- Account name (Nome account)
- ID account
- ARN dell'applicazione
- Application name (Nome applicazione)
- Nome del prodotto (per un prodotto Servizio AWS o un prodotto di terze parti che invia i risultati a Security Hub CSPM)
- Record state (Stato del record)
- Region
- Tag risorsa
- Gravità
- Stato del flusso di lavoro

Per impostazione predefinita, i dati del dashboard vengono filtrati in base ai seguenti criteri: `Workflow.Status` è `NOTIFIED` o`NEW`, ed è. `RecordState` `ACTIVE` Questi criteri vengono visualizzati sopra la dashboard, sotto la casella del filtro. Per rimuovere questi criteri, scegli X nel token di filtro relativo ai criteri che desideri rimuovere.

Se applichi criteri di filtro che desideri utilizzare nuovamente, puoi salvarli come set di filtri. Un set di filtri è un insieme di criteri di filtro che crei e salvi per riapplicare quando esaminate i dati nella dashboard di riepilogo. È possibile creare e salvare un set di filtri che utilizza uno qualsiasi dei campi disponibili tranne i seguenti campi: ARN dell'applicazione, nome dell'applicazione e tag della risorsa.

Creazione e salvataggio di set di filtri

Segui questi passaggi per creare e salvare un set di filtri.

Per creare e salvare un set di filtri

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Riepilogo.
3. Nella casella del filtro sopra la dashboard di riepilogo, inserisci i criteri di filtro per il set di filtri.
4. Nel menu Cancella filtri, scegli Salva nuovo set di filtri.
5. Nella finestra di dialogo Salva set di filtri, inserite un nome per il set di filtri.
6. (Facoltativo) Per utilizzare il filtro impostato di default ogni volta che aprite la pagina di riepilogo, selezionate l'opzione per impostarlo come visualizzazione predefinita.
7. Selezionare Salva.

Per passare da un set di filtri che hai creato a uno salvato, utilizza il menu Scegli un set di filtri sopra la dashboard di riepilogo. Quando si seleziona un set di filtri, Security Hub CSPM applica i criteri del set di filtri ai dati sulla dashboard.

Aggiornamento o eliminazione dei set di filtri

Segui questi passaggi per aggiornare o eliminare un set di filtri esistente. Se si elimina un set di filtri attualmente impostato come visualizzazione predefinita del dashboard di riepilogo, la visualizzazione predefinita viene ripristinata sulla visualizzazione CSPM predefinita di Security Hub.

Per aggiornare o eliminare un set di filtri

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Riepilogo.
3. Nel menu Scegli un set di filtri sopra la pagina di riepilogo, scegli il set di filtri.
4. Nel menu Cancella filtri, effettuate una delle seguenti operazioni:
   - Per aggiornare il set di filtri, scegliete Aggiorna il set di filtri corrente. Quindi, inserisci le modifiche nella finestra di dialogo che appare.

- Per eliminare il set di filtri, scegliete Elimina il set di filtri corrente. Quindi, scegliete Elimina nella finestra di dialogo che appare.

Personalizzazione della dashboard di riepilogo in Security Hub CSPM

È possibile personalizzare la dashboard di riepilogo sulla console CSPM di Security Hub in diversi modi. Ad esempio, puoi aggiungere e rimuovere widget dalla dashboard. Puoi anche riorganizzare e ridimensionare i widget sulla dashboard. Per un elenco dei widget disponibili e una descrizione di ciascuno di essi, consulta. Widget disponibili per la dashboard di riepilogo

Se personalizzi la dashboard, Security Hub CSPM applica immediatamente le modifiche e salva le nuove impostazioni della dashboard. Le modifiche si applicano alla visualizzazione della dashboard in tutti Regioni AWS i browser.

Per personalizzare il Riepilogo pannello di controllo

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, scegli Riepilogo.
3. Effettua una delle seguenti operazioni:

   - Per aggiungere un widget, scegli Aggiungi widget nell'angolo in alto a destra della pagina. Nella barra di ricerca, inserisci il titolo del widget da aggiungere. Quindi, trascina il widget nella posizione desiderata.
   - Per rimuovere un widget, scegli i tre punti nell'angolo in alto a destra del widget.
   - Per spostare un widget, scegli la maniglia nell'angolo superiore sinistro del widget, quindi trascina il widget nella posizione desiderata.
   - Per modificare le dimensioni di un widget, scegli la maniglia di ridimensionamento nell'angolo inferiore destro del widget. Trascina il bordo del widget fino a raggiungere la dimensione desiderata.

Per ripristinare successivamente le impostazioni originali, scegli Ripristina il layout predefinito nella parte superiore della pagina.

Limiti regionali per Security Hub CSPM

Alcune funzionalità CSPM di AWS Security Hub sono disponibili solo in alcuni casi. Regioni AWS Le seguenti sezioni specificano questi limiti regionali. Per un elenco completo di tutte le regioni in cui Security Hub CSPM è attualmente disponibile, consulta Endpoint e quote AWS di Security Hub in. Riferimenti generali di AWS

Cross-Region restrizioni di aggregazione

InAWS GovCloud (US) Regions, l'aggregazione interregionale è disponibile solo per i risultati, gli aggiornamenti di ricerca e le informazioni approfondite. AWS GovCloud (US) Regions In particolare, puoi aggregare i risultati, trovare aggiornamenti e approfondimenti solo tra le regioni AWS GovCloud (US-East) e AWS GovCloud (US-West).

Nelle regioni della Cina, l'aggregazione interregionale è disponibile per i risultati, gli aggiornamenti delle ricerche e gli approfondimenti solo nelle regioni della Cina. In particolare, puoi aggregare risultati, trovare aggiornamenti e approfondimenti solo tra le regioni Cina (Pechino) e Cina (Ningxia).

Non puoi utilizzare una regione disattivata per impostazione predefinita come regione di aggregazione. Per un elenco delle aree che sono disabilitate per impostazione predefinita, consulta Attivare o disattivare Regioni AWS nel proprio account nella Guida Gestione dell'account AWS di riferimento.

Disponibilità di integrazioni per regione

Alcune integrazioni non sono disponibili in tutte. Regioni AWS Nella console Security Hub CSPM, un'integrazione non viene visualizzata nella pagina Integrazioni se non è disponibile nella regione a cui hai attualmente effettuato l'accesso.

Integrazioni supportate nelle regioni Cina (Pechino) e Cina (Ningxia)

Nelle regioni Cina (Pechino) e Cina (Ningxia), Security Hub CSPM supporta solo le seguenti integrazioni con: Servizi AWS

- 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 ManagerGestore di patch

Nelle regioni Cina (Pechino) e Cina (Ningxia), Security Hub CSPM supporta solo le seguenti integrazioni di terze parti:

- 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

Integrazioni supportate inAWS GovCloud (US-East)andAWS GovCloud (US-West)Regioni

Nelle AWS GovCloud (US-West) regioni AWS GovCloud (US-East) e, Security Hub CSPM supporta solo le seguenti integrazioni con: Servizi AWS

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health

- Sistema di analisi degli accessi IAM
- Amazon Inspector
- AWS IoT Device Defender

Nelle AWS GovCloud (US-West) regioni AWS GovCloud (US-East) e, Security Hub CSPM supporta solo le seguenti integrazioni di terze parti:

- 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(disponibile solo in AWS GovCloud (US-West))
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer

- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Disponibilità degli standard per regione

Lo standard AWS Control Tower gestito dai servizi è disponibile solo nei seguenti Regioni AWS supportiAWS Control Tower. Per un elenco delle regioni AWS Control Tower attualmente supportate, consulta How Regioni AWS Work With AWS Control Tower nella Guida per l'AWS Control Towerutente.

Lo standard AWS Resource Tagging non è disponibile nella regione Asia Pacifico (Taipei).

Altri standard di sicurezza sono disponibili in tutte le regioni in cui è attualmente disponibile Security Hub CSPM.

Disponibilità dei controlli per regione

Alcuni controlli CSPM di Security Hub non sono disponibili in tutti. Regioni AWS Per un elenco dei controlli che non sono disponibili in ogni regione, vedi. Limiti regionali sui controlli CSPM di Security Hub

Nella console CSPM di Security Hub, un controllo non viene visualizzato nell'elenco dei controlli se non è disponibile nella regione a cui hai attualmente effettuato l'accesso. L'eccezione è una regione di aggregazione. Se imposti una regione di aggregazione e accedi a quella regione, la console mostra i controlli disponibili nella regione di aggregazione o in una o più aree collegate.

Limiti regionali sui controlli CSPM di Security Hub

Alcuni controlli CSPM di AWS Security Hub non sono disponibili in tutti. Regioni AWS Questa pagina specifica quali controlli non sono disponibili in regioni specifiche.

Nella console CSPM di Security Hub, un controllo non viene visualizzato nell'elenco dei controlli se non è disponibile nella regione a cui hai attualmente effettuato l'accesso. L'eccezione è una regione di aggregazione. Se imposti una regione di aggregazione e accedi a quella regione, la console mostra i controlli disponibili nella regione di aggregazione o in una o più aree collegate.

Regioni AWS

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- Stati Uniti occidentali (California settentrionale)
- Stati Uniti occidentali (Oregon)
- Africa (Città del Capo)
- Asia Pacifico (Hong Kong)
- Asia Pacifico (Hyderabad)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Malesia)
- Asia Pacifico (Melbourne)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Nuova Zelanda)
- Asia Pacifico (Osaka)
- Asia Pacifico (Seul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Taipei)
- Asia Pacifico (Thailandia)
- Asia Pacifico (Tokyo)
- Canada (Centrale)
- Canada occidentale (Calgary)
- Cina (Pechino)
- Cina (Ningxia)
- Europa (Francoforte)
- Europa (Irlanda)
- Europa (Londra)
- Europa (Milano)
- Europa (Parigi)

- Europa (Spagna)
- Europa (Stoccolma)
- Europa (Zurigo)
- Israele (Tel Aviv)
- Messico (centrale)
- Medio Oriente (Bahrein)
- Medio Oriente (Emirati Arabi Uniti)
- Sud America (San Paolo)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

Stati Uniti orientali (Virginia settentrionale)

I seguenti controlli non sono supportati nella regione Stati Uniti orientali (Virginia settentrionale).

- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate

Stati Uniti orientali (Ohio)

I seguenti controlli non sono supportati nella regione Stati Uniti orientali (Ohio).

- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato

- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate

- [IVS.3] I canali IVS devono essere etichettati
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Stati Uniti occidentali (California settentrionale)

I seguenti controlli non sono supportati nella regione Stati Uniti occidentali (California settentrionale).

- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata

- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch

- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato

- [RDS.47] I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.48] I cluster RDS per MySQL DB devono essere configurati per copiare i tag nelle istantanee del DB
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Stati Uniti occidentali (Oregon)

I seguenti controlli non sono supportati nella regione Stati Uniti occidentali (Oregon).

- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS

- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Africa (Città del Capo)

I seguenti controlli non sono supportati nella regione Africa (Città del Capo).

- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati

- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati

- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati

- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [ES.3] I domini Elasticsearch devono crittografare i dati inviati tra i nodi
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate

- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [RDS.1] L'istantanea RDS deve essere privata
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container

- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Asia Pacifico (Hong Kong)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Hong Kong).

- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys

- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata

- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati

- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SES.1] Gli elenchi di contatti SES devono essere etichettati
- [SES.2] I set di configurazione SES devono essere etichettati
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Asia Pacifico (Hyderabad)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Hyderabad).

- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato

- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico
- [CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.2] I certificati DMS devono essere etichettati

- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate
- [EC2.40] I gateway NAT EC2 devono essere etichettati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager

- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata

- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate

- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MQ.4] I broker Amazon MQ devono essere etichettati
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby

- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato

- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate

- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata

- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Asia Pacifico (Giacarta)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Giacarta).

- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica

- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili
- [CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato
- [CodeBuild.3] I log CodeBuild S3 devono essere crittografati
- [CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]

- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch

- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato

- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate

- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati

- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola

- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Asia Pacifico (Malesia)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Malesia).

- [ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato
- [ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- [Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata
- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [Athena.4] I gruppi di lavoro Athena dovrebbero avere la registrazione abilitata
- [AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità

- [AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)
- [AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità
- [AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [Backup.2] AWS Backup i punti di ripristino devono essere etichettati
- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.2] Le politiche di pianificazione dei batch devono essere etichettate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito

- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico
- [CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
- [CloudTrail.10] I data store di eventi di CloudTrail Lake devono essere crittografati con Customer Managed AWS KMS keys
- [CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili
- [CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato
- [CodeBuild.3] I log CodeBuild S3 devono essere crittografati
- [CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]

- [CodeBuild.7] le esportazioni dei gruppi di CodeBuild report devono essere crittografate quando sono inattive
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate
- [Cognito.4] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata
- [Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito
- [Cognito.6] I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [DataSync.1] DataSync le attività dovrebbero avere la registrazione abilitata
- [DataSync.2] le DataSync attività devono essere etichettate
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL

- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup
- [DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup
- [EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate

- [EC2.40] I gateway NAT EC2 devono essere etichettati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto
- [EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server
- [EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR
- [EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry
- [EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.174] I set di opzioni DHCP EC2 devono essere etichettati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2
- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag
- [ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata

- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ECR.5] I repository ECR devono essere crittografati e gestiti dal cliente AWS KMS keys
- [ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host
- [ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati
- [ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root
- [ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore
- [ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione
- [ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate
- [ECS.12] I cluster ECS devono utilizzare Container Insights
- [ECS.17] Le definizioni delle attività ECS non devono utilizzare la modalità di rete host
- [ECS.19] I provider di capacità ECS dovrebbero avere abilitato la protezione gestita dalle terminazioni
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio
- [EFS.7] I file system EFS devono avere i backup automatici abilitati
- [EFS.8] I file system EFS devono essere crittografati quando sono inattivi
- [EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata
- [EKS.7] Le configurazioni dei provider di identità EKS devono essere contrassegnate
- [EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata
- [ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità
- [ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa

- [ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo
- [EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [ES.9] I domini Elasticsearch devono essere etichettati
- [EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata

- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ
- [FSx.4] I file system FSx for NetApp ONTAP devono essere configurati per l'implementazione Multi-AZ
- [FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.1] AWS Glue i lavori devono essere etichettati
- [Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato
- [GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato
- [GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata
- [GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata
- [GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate

- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
- [IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
- [IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
- [IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
- [IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
- [IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
- [IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata

- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi
- [Kinesis.3] I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [KMS.5] Le chiavi KMS non devono essere accessibili al pubblico
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch

- [MQ.4] I broker Amazon MQ devono essere etichettati
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker
- [MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata

- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata
- [PCA.2] AWS Le autorità di certificazione CA private devono essere contrassegnate
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.26] Le istanze DB RDS devono essere protette da un piano di backup
- [RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.36] Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch
- [RDS.38] Le istanze DB RDS per PostgreSQL devono essere crittografate in transito

- [RDS.39] Le istanze DB RDS per MySQL devono essere crittografate in transito
- [RDS.40] Le istanze DB di RDS per SQL Server devono pubblicare i log in Logs CloudWatch
- [RDS.41] Le istanze DB di RDS per SQL Server devono essere crittografate in transito
- [RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch
- [] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43
- [RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [RDS.46] Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso gateway Internet
- [RDS.47] I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata
- [Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate
- [Redshift.16] I gruppi di sottoreti del cluster Redshift devono avere sottoreti provenienti da più zone di disponibilità
- [Redshift.17] I gruppi di parametri del cluster Redshift devono essere etichettati
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito

- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni
- [S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita
- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- [S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3
- [S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita
- [S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata
- [S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto
- [S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container

- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.4] I documenti SSM non devono essere pubblici
- [SSM.5] I documenti SSM devono essere etichettati
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata

- [StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata
- [Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [Transfer.5] I certificati Transfer Family devono essere etichettati
- [Transfer.6] I connettori Transfer Family devono essere etichettati
- [Transfer.7] I profili Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Asia Pacifico (Melbourne)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Melbourne).

- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati

- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata
- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS

- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL

- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate
- [EC2.40] I gateway NAT EC2 devono essere etichettati
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts

- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici

- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
- [IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
- [IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
- [IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
- [IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
- [IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
- [IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno

- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati

- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch

- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [RDS.1] L'istantanea RDS deve essere privata
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate

- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore

- [SES.1] Gli elenchi di contatti SES devono essere etichettati
- [SES.2] I set di configurazione SES devono essere etichettati
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.4] I documenti SSM non devono essere pubblici
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Asia Pacifico (Mumbai)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Mumbai).

- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS

- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati

- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Asia Pacifico (Nuova Zelanda)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Nuova Zelanda).

- [ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato
- [ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- [Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.1] API Gateway REST e la registrazione dell'esecuzione dell' WebSocket API devono essere abilitati
- [APIGateway.2] Le fasi API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend
- [APIGateway.3] Le fasi API REST di API Gateway dovrebbero avere AWS X-Ray tracciamento abilitato
- [APIGateway.4] API Gateway deve essere associato a un ACL Web WAF
- [APIGateway.5] I dati della cache dell'API REST di API Gateway devono essere crittografati quando sono inattivi
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione

- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [APIGateway.10] Le integrazioni API Gateway V2 devono utilizzare HTTPS per le connessioni private
- [APIGateway.11] I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata
- [AppSync.4] AWS AppSync Le API GraphQL devono essere etichettate
- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [Athena.2] I cataloghi di dati Athena devono essere etichettati
- [Athena.3] I gruppi di lavoro Athena devono essere etichettati
- [Athena.4] I gruppi di lavoro Athena dovrebbero avere la registrazione abilitata
- [AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità
- [AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)
- [AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità
- [AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [Backup.2] AWS Backup i punti di ripristino devono essere etichettati
- [Backup.4] AWS Backup i piani di report devono essere etichettati

- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.2] Le politiche di pianificazione dei batch devono essere etichettate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti

- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico
- [CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
- [CloudTrail.10] I data store di eventi di CloudTrail Lake devono essere crittografati con Customer Managed AWS KMS keys
- [CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili
- [CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato
- [CodeBuild.3] I log CodeBuild S3 devono essere crittografati
- [CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]
- [CodeBuild.7] le esportazioni dei gruppi di CodeBuild report devono essere crittografate quando sono inattive
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate

- [Cognito.4] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata
- [Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito
- [Cognito.6] I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [DataSync.1] DataSync le attività dovrebbero avere la registrazione abilitata
- [DataSync.2] le DataSync attività devono essere etichettate
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche

- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup
- [DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup
- [EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate
- [EC2.40] I gateway NAT EC2 devono essere etichettati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto
- [EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server
- [EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR
- [EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry
- [EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts

- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata
- [EC2.172] Le impostazioni VPC Block Public Access di EC2 dovrebbero bloccare il traffico del gateway Internet
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.174] I set di opzioni DHCP EC2 devono essere etichettati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.182] Le impostazioni di blocco dell'accesso pubblico devono essere abilitate per gli snapshot di Amazon EBS
- [EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2
- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag
- [ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ECR.5] I repository ECR devono essere crittografati e gestiti dal cliente AWS KMS keys
- [ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host
- [ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati
- [ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root
- [ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore

- [ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione
- [ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate
- [ECS.12] I cluster ECS devono utilizzare Container Insights
- [ECS.16] I set di attività ECS non devono assegnare automaticamente indirizzi IP pubblici
- [ECS.17] Le definizioni delle attività ECS non devono utilizzare la modalità di rete host
- [ECS.18] Le definizioni delle attività ECS devono utilizzare la crittografia in transito per i volumi EFS
- [ECS.19] I provider di capacità ECS dovrebbero avere abilitato la protezione gestita dalle terminazioni
- [ECS.20] Le definizioni delle attività ECS devono configurare gli utenti non root nelle definizioni dei container Linux
- [ECS.21] Le definizioni delle attività ECS devono configurare gli utenti non amministratori nelle definizioni dei contenitori Windows
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio
- [EFS.7] I file system EFS devono avere i backup automatici abilitati
- [EFS.8] I file system EFS devono essere crittografati quando sono inattivi
- [EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata
- [EKS.7] Le configurazioni dei provider di identità EKS devono essere contrassegnate
- [EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata
- [EKS.9] I gruppi di nodi EKS devono essere eseguiti su una versione di Kubernetes supportata
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità
- [ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa

- [ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.16] Application Load Balancers deve essere associato a un AWS WAF ACL Web
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- [ELB.21] I gruppi target di Application e Network Load Balancer devono utilizzare protocolli di controllo dello stato crittografati
- [ELB.22] I gruppi target ELB devono utilizzare protocolli di trasporto crittografati
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo
- [EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito
- [ES.3] I domini Elasticsearch devono crittografare i dati inviati tra i nodi

- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [ES.9] I domini Elasticsearch devono essere etichettati
- [EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ
- [FSx.4] I file system FSx for NetApp ONTAP devono essere configurati per l'implementazione Multi-AZ
- [FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.1] AWS Glue i lavori devono essere etichettati
- [Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.1] GuardDuty dovrebbe essere abilitato
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [GuardDuty.3] Gli GuardDuty IPSets devono essere etichettati
- [GuardDuty.4] i GuardDuty rilevatori devono essere etichettati
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato
- [GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato

- [GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata
- [GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata
- [GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
- [IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
- [IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
- [IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
- [IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
- [IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
- [IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi

- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate

- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi
- [Kinesis.3] I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [KMS.5] Le chiavi KMS non devono essere accessibili al pubblico
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MQ.4] I broker Amazon MQ devono essere etichettati
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker
- [MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati

- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata

- [PCA.2] AWS Le autorità di certificazione CA private devono essere contrassegnate
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.26] Le istanze DB RDS devono essere protette da un piano di backup
- [RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.36] Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch
- [RDS.38] Le istanze DB RDS per PostgreSQL devono essere crittografate in transito
- [RDS.39] Le istanze DB RDS per MySQL devono essere crittografate in transito
- [RDS.40] Le istanze DB di RDS per SQL Server devono pubblicare i log in Logs CloudWatch
- [RDS.41] Le istanze DB di RDS per SQL Server devono essere crittografate in transito
- [RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch
- [] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43
- [RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [RDS.46] Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso gateway Internet
- [RDS.47] I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.48] I cluster RDS per MySQL DB devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.50] I cluster RDS DB devono avere un periodo di conservazione dei backup sufficiente
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata

- [Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico
- [Redshift.3] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate
- [Redshift.4] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata
- [Redshift.6] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati
- [Redshift.7] I cluster Redshift devono utilizzare un routing VPC avanzato
- [Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.11] I cluster Redshift devono essere etichettati
- [Redshift.13] Le istantanee del cluster Redshift devono essere etichettate
- [Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate
- [Redshift.16] I gruppi di sottoreti del cluster Redshift devono avere sottoreti provenienti da più zone di disponibilità
- [Redshift.17] I gruppi di parametri del cluster Redshift devono essere etichettati
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni

- [S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita
- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- [S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3
- [S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita
- [S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata
- [S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto
- [S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato

- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.1] Gli elenchi di contatti SES devono essere etichettati
- [SES.2] I set di configurazione SES devono essere etichettati
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.1] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager
- [SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch
- [SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT
- [SSM.4] I documenti SSM non devono essere pubblici
- [SSM.5] I documenti SSM devono essere etichettati
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata

- [StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata
- [Transfer.1] AWS Transfer Family i flussi di lavoro devono essere etichettati
- [Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [Transfer.5] I certificati Transfer Family devono essere etichettati
- [Transfer.6] I connettori Transfer Family devono essere etichettati
- [Transfer.7] I profili Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WAF.11] AWS WAF la registrazione ACL web deve essere abilitata
- [WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Asia Pacifico (Osaka)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Osaka).

- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati

- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati

- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati

- [EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR
- [EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry
- [EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati

- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch

- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch
- [SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Asia Pacifico (Seul)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Seoul).

- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato

- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati

- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola

- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Asia Pacifico (Singapore)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Singapore).

- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati

- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Asia Pacifico (Sydney)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Sydney).

- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti

- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Asia Pacifico (Taipei)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Taipei).

- [ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato

- [ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- [ACM.3] I certificati ACM devono essere etichettati
- [Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.1] API Gateway REST e la registrazione dell'esecuzione dell' WebSocket API devono essere abilitati
- [APIGateway.2] Le fasi API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend
- [APIGateway.3] Le fasi API REST di API Gateway dovrebbero avere AWS X-Ray tracciamento abilitato
- [APIGateway.4] API Gateway deve essere associato a un ACL Web WAF
- [APIGateway.5] I dati della cache dell'API REST di API Gateway devono essere crittografati quando sono inattivi
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [APIGateway.10] Le integrazioni API Gateway V2 devono utilizzare HTTPS per le connessioni private
- [APIGateway.11] I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata

- [AppSync.4] AWS AppSync Le API GraphQL devono essere etichettate
- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [Athena.2] I cataloghi di dati Athena devono essere etichettati
- [Athena.3] I gruppi di lavoro Athena devono essere etichettati
- [Athena.4] I gruppi di lavoro Athena dovrebbero avere la registrazione abilitata
- [AutoScaling.1] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB
- [AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità
- [AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)
- [AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità
- [AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2
- [AutoScaling.10] I gruppi EC2 Auto Scaling devono essere etichettati
- [Autoscaling.5] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [Backup.2] AWS Backup i punti di ripristino devono essere etichettati
- [Backup.3] AWS Backup i vault devono essere etichettati
- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [Backup.5] AWS Backup i piani di backup devono essere etichettati
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.2] Le politiche di pianificazione dei batch devono essere etichettate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata

- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.2] gli CloudFormation stack devono essere etichettati
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati

- [CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico
- [CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
- [] CloudTrail.9 i trail devono essere etichettati CloudTrail
- [CloudTrail.10] I data store di eventi di CloudTrail Lake devono essere crittografati con Customer Managed AWS KMS keys
- [CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili
- [CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato
- [CodeBuild.3] I log CodeBuild S3 devono essere crittografati
- [CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]
- [CodeBuild.7] le esportazioni dei gruppi di CodeBuild report devono essere crittografate quando sono inattive
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate
- [Cognito.4] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata
- [Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito
- [Cognito.6] I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati

- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [DataSync.1] DataSync le attività dovrebbero avere la registrazione abilitata
- [DataSync.2] le DataSync attività devono essere etichettate
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.1] Le istanze di replica del Database Migration Service non devono essere pubbliche
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata

- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup
- [DynamoDB.5] Le tabelle DynamoDB devono essere etichettate
- [DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.10] Amazon EC2 deve essere configurato per utilizzare gli endpoint VPC creati per il servizio Amazon EC2
- [EC2.19] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio
- [EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup
- [EC2.33] Gli allegati del gateway di transito EC2 devono essere etichettati
- [EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate
- [EC2.35] Le interfacce di rete EC2 devono essere etichettate
- [EC2.36] I gateway per i clienti EC2 devono essere etichettati
- [EC2.37] Gli indirizzi IP elastici EC2 devono essere etichettati
- [EC2.38] Le istanze EC2 devono essere etichettate
- [EC2.39] I gateway Internet EC2 devono essere etichettati
- [EC2.40] I gateway NAT EC2 devono essere etichettati
- [EC2.41] Gli ACL di rete EC2 devono essere etichettati
- [EC2.42] Le tabelle delle rotte EC2 devono essere etichettate

- [EC2.43] I gruppi di sicurezza EC2 devono essere etichettati
- [EC2.44] Le sottoreti EC2 devono essere etichettate
- [EC2.45] I volumi EC2 devono essere etichettati
- [EC2.46] I VPC Amazon devono essere etichettati
- [EC2.47] I servizi endpoint Amazon VPC devono essere etichettati
- [EC2.48] I log di flusso di Amazon VPC devono essere etichettati
- [EC2.49] Le connessioni peering Amazon VPC devono essere etichettate
- [EC2.50] I gateway VPN EC2 devono essere etichettati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.52] I gateway di transito EC2 devono essere etichettati
- [EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto
- [EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server
- [EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR
- [EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry
- [EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata
- [EC2.172] Le impostazioni VPC Block Public Access di EC2 dovrebbero bloccare il traffico del gateway Internet
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.174] I set di opzioni DHCP EC2 devono essere etichettati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati

- [EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.182] Le impostazioni di blocco dell'accesso pubblico devono essere abilitate per gli snapshot di Amazon EBS
- [EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2
- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag
- [ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ECR.5] I repository ECR devono essere crittografati e gestiti dal cliente AWS KMS keys
- [ECS.2] Ai servizi ECS non dovrebbero essere assegnati automaticamente indirizzi IP pubblici
- [ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host
- [ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati
- [ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root
- [ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore
- [ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione
- [ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate
- [ECS.12] I cluster ECS devono utilizzare Container Insights
- [ECS.13] I servizi ECS devono essere etichettati
- [ECS.14] I cluster ECS devono essere etichettati
- [ECS.15] Le definizioni delle attività ECS devono essere contrassegnate
- [ECS.16] I set di attività ECS non devono assegnare automaticamente indirizzi IP pubblici
- [ECS.17] Le definizioni delle attività ECS non devono utilizzare la modalità di rete host

- [ECS.18] Le definizioni delle attività ECS devono utilizzare la crittografia in transito per i volumi EFS
- [ECS.19] I provider di capacità ECS dovrebbero avere abilitato la protezione gestita dalle terminazioni
- [ECS.20] Le definizioni delle attività ECS devono configurare gli utenti non root nelle definizioni dei container Linux
- [ECS.21] Le definizioni delle attività ECS devono configurare gli utenti non amministratori nelle definizioni dei contenitori Windows
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EFS.5] I punti di accesso EFS devono essere etichettati
- [EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio
- [EFS.7] I file system EFS devono avere i backup automatici abilitati
- [EFS.8] I file system EFS devono essere crittografati quando sono inattivi
- [EKS.1] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico
- [EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata
- [EKS.6] I cluster EKS devono essere etichettati
- [EKS.7] Le configurazioni dei provider di identità EKS devono essere contrassegnate
- [EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata
- [EKS.9] I gruppi di nodi EKS devono essere eseguiti su una versione di Kubernetes supportata
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [ELB.3] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS
- [ELB.7] I Classic Load Balancer dovrebbero avere abilitato il drenaggio della connessione
- [ELB.8] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita che sia solida AWS Config Durata
- [ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità

- [ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.16] Application Load Balancers deve essere associato a un AWS WAF ACL Web
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- [ELB.21] I gruppi target di Application e Network Load Balancer devono utilizzare protocolli di controllo dello stato crittografati
- [ELB.22] I gruppi target ELB devono utilizzare protocolli di trasporto crittografati
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo

- [EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito
- [ES.1] I domini Elasticsearch devono avere la crittografia a riposo abilitata
- [ES.2] I domini Elasticsearch non devono essere accessibili al pubblico
- [ES.3] I domini Elasticsearch devono crittografare i dati inviati tra i nodi
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [ES.5] I domini Elasticsearch devono avere la registrazione di controllo abilitata
- [ES.6] I domini Elasticsearch devono avere almeno tre nodi di dati
- [ES.7] I domini Elasticsearch devono essere configurati con almeno tre nodi master dedicati
- [ES.8] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS
- [ES.9] I domini Elasticsearch devono essere etichettati
- [EventBridge.2] i bus EventBridge degli eventi devono essere etichettati
- [EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ
- [FSx.4] I file system FSx for NetApp ONTAP devono essere configurati per l'implementazione Multi-AZ
- [FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.1] AWS Glue i lavori devono essere etichettati

- [Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.1] GuardDuty dovrebbe essere abilitato
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [GuardDuty.3] Gli GuardDuty IPSets devono essere etichettati
- [GuardDuty.4] i GuardDuty rilevatori devono essere etichettati
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato
- [GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato
- [GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata
- [GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata
- [GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
- [IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola

- [IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
- [IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
- [IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
- [IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
- [IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.23] Gli analizzatori IAM Access Analyzer devono essere etichettati
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati

- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi
- [Kinesis.2] Gli stream Kinesis devono essere etichettati
- [Kinesis.3] I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [KMS.3] AWS KMS keys non devono essere eliminati involontariamente
- [KMS.5] Le chiavi KMS non devono essere accessibili al pubblico
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Lambda.6] Le funzioni Lambda devono essere etichettate
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato

- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MQ.4] I broker Amazon MQ devono essere etichettati
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker
- [MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.7] I firewall Network Firewall devono essere etichettati

- [NetworkFirewall.8] Le politiche firewall di Network Firewall devono essere etichettate
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata
- [PCA.2] AWS Le autorità di certificazione CA private devono essere contrassegnate
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.16] I cluster Aurora DB devono essere configurati per copiare i tag nelle istantanee DB
- [RDS.17] Le istanze DB RDS devono essere configurate per copiare i tag negli snapshot
- [RDS.19] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici del cluster
- [RDS.20] Le sottoscrizioni esistenti per le notifiche degli eventi RDS devono essere configurate per gli eventi critici delle istanze di database
- [RDS.21] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database
- [RDS.22] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database

- [RDS.23] Le istanze RDS non devono utilizzare una porta predefinita del motore di database
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.26] Le istanze DB RDS devono essere protette da un piano di backup
- [RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi
- [RDS.28] I cluster RDS DB devono essere etichettati
- [RDS.29] Gli snapshot del cluster RDS DB devono essere etichettati
- [RDS.30] Le istanze DB RDS devono essere etichettate
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RDS.32] Gli snapshot RDS DB devono essere etichettati
- [RDS.33] I gruppi di sottoreti RDS DB devono essere etichettati
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.36] Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch
- [RDS.38] Le istanze DB RDS per PostgreSQL devono essere crittografate in transito
- [RDS.39] Le istanze DB RDS per MySQL devono essere crittografate in transito
- [RDS.40] Le istanze DB di RDS per SQL Server devono pubblicare i log in Logs CloudWatch
- [RDS.41] Le istanze DB di RDS per SQL Server devono essere crittografate in transito
- [RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch
- [] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43
- [RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [RDS.46] Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso gateway Internet
- [RDS.47] I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB

- [RDS.48] I cluster RDS per MySQL DB devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.50] I cluster RDS DB devono avere un periodo di conservazione dei backup sufficiente
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata
- [Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico
- [Redshift.2] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito
- [Redshift.3] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate
- [Redshift.4] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata
- [Redshift.6] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati
- [Redshift.7] I cluster Redshift devono utilizzare un routing VPC avanzato
- [Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.11] I cluster Redshift devono essere etichettati
- [Redshift.12] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate
- [Redshift.13] Le istantanee del cluster Redshift devono essere etichettate
- [Redshift.14] I gruppi di sottoreti del cluster Redshift devono essere etichettati
- [Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate
- [Redshift.16] I gruppi di sottoreti del cluster Redshift devono avere sottoreti provenienti da più zone di disponibilità
- [Redshift.17] I gruppi di parametri del cluster Redshift devono essere etichettati
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys

- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni
- [S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita
- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- [S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3
- [S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita
- [S3.17] I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys
- [S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata
- [S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto
- [S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate

- [SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.1] Gli elenchi di contatti SES devono essere etichettati
- [SES.2] I set di configurazione SES devono essere etichettati
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [SecretsManager.1] I segreti di Secrets Manager devono avere la rotazione automatica abilitata
- [SecretsManager.2] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente
- [SecretsManager.3] Rimuovi i segreti inutilizzati di Secrets Manager
- [SecretsManager.4] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni

- [SecretsManager.5] I segreti di Secrets Manager devono essere etichettati
- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SNS.3] Gli argomenti SNS devono essere etichettati
- [SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.1] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager
- [SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch
- [SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT
- [SSM.4] I documenti SSM non devono essere pubblici
- [SSM.5] I documenti SSM devono essere etichettati
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata
- [StepFunctions.2] Le attività di Step Functions devono essere etichettate
- [Transfer.1] AWS Transfer Family i flussi di lavoro devono essere etichettati
- [Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [Transfer.5] I certificati Transfer Family devono essere etichettati
- [Transfer.6] I connettori Transfer Family devono essere etichettati
- [Transfer.7] I profili Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola

- [WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WAF.11] AWS WAF la registrazione ACL web deve essere abilitata
- [WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Asia Pacifico (Thailandia)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Tailandia).

- [ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato
- [ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- [Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [APIGateway.10] Le integrazioni API Gateway V2 devono utilizzare HTTPS per le connessioni private
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati

- [AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata
- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [Athena.2] I cataloghi di dati Athena devono essere etichettati
- [Athena.3] I gruppi di lavoro Athena devono essere etichettati
- [Athena.4] I gruppi di lavoro Athena dovrebbero avere la registrazione abilitata
- [AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità
- [AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)
- [AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità
- [AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [Backup.2] AWS Backup i punti di ripristino devono essere etichettati
- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.2] Le politiche di pianificazione dei batch devono essere etichettate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys

- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico
- [CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail

- [CloudTrail.10] I data store di eventi di CloudTrail Lake devono essere crittografati con Customer Managed AWS KMS keys
- [CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili
- [CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato
- [CodeBuild.3] I log CodeBuild S3 devono essere crittografati
- [CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]
- [CodeBuild.7] le esportazioni dei gruppi di CodeBuild report devono essere crittografate quando sono inattive
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate
- [Cognito.4] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata
- [Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito
- [Cognito.6] I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [DataSync.1] DataSync le attività dovrebbero avere la registrazione abilitata
- [DataSync.2] le DataSync attività devono essere etichettate
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati

- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup
- [DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito

- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup
- [EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate
- [EC2.40] I gateway NAT EC2 devono essere etichettati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto
- [EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server
- [EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR
- [EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry
- [EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata
- [EC2.172] Le impostazioni VPC Block Public Access di EC2 dovrebbero bloccare il traffico del gateway Internet
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.174] I set di opzioni DHCP EC2 devono essere etichettati

- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.182] Le impostazioni di blocco dell'accesso pubblico devono essere abilitate per gli snapshot di Amazon EBS
- [EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2
- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag
- [ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ECR.5] I repository ECR devono essere crittografati e gestiti dal cliente AWS KMS keys
- [ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host
- [ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati
- [ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root
- [ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore
- [ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione
- [ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate
- [ECS.12] I cluster ECS devono utilizzare Container Insights
- [ECS.16] I set di attività ECS non devono assegnare automaticamente indirizzi IP pubblici
- [ECS.17] Le definizioni delle attività ECS non devono utilizzare la modalità di rete host
- [ECS.18] Le definizioni delle attività ECS devono utilizzare la crittografia in transito per i volumi EFS
- [ECS.19] I provider di capacità ECS dovrebbero avere abilitato la protezione gestita dalle terminazioni

- [ECS.20] Le definizioni delle attività ECS devono configurare gli utenti non root nelle definizioni dei container Linux
- [ECS.21] Le definizioni delle attività ECS devono configurare gli utenti non amministratori nelle definizioni dei contenitori Windows
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio
- [EFS.7] I file system EFS devono avere i backup automatici abilitati
- [EFS.8] I file system EFS devono essere crittografati quando sono inattivi
- [EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata
- [EKS.7] Le configurazioni dei provider di identità EKS devono essere contrassegnate
- [EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata
- [EKS.9] I gruppi di nodi EKS devono essere eseguiti su una versione di Kubernetes supportata
- [ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità
- [ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati

- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo
- [EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [ES.9] I domini Elasticsearch devono essere etichettati
- [EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ
- [FSx.4] I file system FSx for NetApp ONTAP devono essere configurati per l'implementazione Multi-AZ

- [FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.1] AWS Glue i lavori devono essere etichettati
- [Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.1] GuardDuty dovrebbe essere abilitato
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato
- [GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato
- [GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata
- [GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata
- [GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide

- [IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
- [IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
- [IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
- [IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
- [IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
- [IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
- [IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati

- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi
- [Kinesis.3] I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [KMS.5] Le chiavi KMS non devono essere accessibili al pubblico
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MQ.4] I broker Amazon MQ devono essere etichettati
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby

- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker
- [MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico

- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata
- [PCA.2] AWS Le autorità di certificazione CA private devono essere contrassegnate
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.26] Le istanze DB RDS devono essere protette da un piano di backup
- [RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.36] Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch
- [RDS.38] Le istanze DB RDS per PostgreSQL devono essere crittografate in transito
- [RDS.39] Le istanze DB RDS per MySQL devono essere crittografate in transito
- [RDS.40] Le istanze DB di RDS per SQL Server devono pubblicare i log in Logs CloudWatch

- [RDS.41] Le istanze DB di RDS per SQL Server devono essere crittografate in transito
- [RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch
- [] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43
- [RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [RDS.46] Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso gateway Internet
- [RDS.47] I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.48] I cluster RDS per MySQL DB devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata
- [Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate
- [Redshift.16] I gruppi di sottoreti del cluster Redshift devono avere sottoreti provenienti da più zone di disponibilità
- [Redshift.17] I gruppi di parametri del cluster Redshift devono essere etichettati
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito

- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni
- [S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita
- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- [S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3
- [S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita
- [S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata
- [S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto
- [S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container

- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.1] Gli elenchi di contatti SES devono essere etichettati
- [SES.2] I set di configurazione SES devono essere etichettati
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT

- [SSM.4] I documenti SSM non devono essere pubblici
- [SSM.5] I documenti SSM devono essere etichettati
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata
- [Transfer.1] AWS Transfer Family i flussi di lavoro devono essere etichettati
- [Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [Transfer.5] I certificati Transfer Family devono essere etichettati
- [Transfer.6] I connettori Transfer Family devono essere etichettati
- [Transfer.7] I profili Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Asia Pacifico (Tokyo)

I seguenti controlli non sono supportati nella regione Asia Pacifico (Tokyo).

- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati

- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Canada (Centrale)

I seguenti controlli non sono supportati nella regione Canada (Centrale).

- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata

- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate

- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Kinesis.3] I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Canada occidentale (Calgary)

I seguenti controlli non sono supportati nella regione Canada occidentale (Calgary).

- [ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato
- [ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- [Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati

- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata
- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [Athena.4] I gruppi di lavoro Athena dovrebbero avere la registrazione abilitata
- [AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità
- [AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)
- [AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità
- [AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys

- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico
- [CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
- [CloudTrail.10] I data store di eventi di CloudTrail Lake devono essere crittografati con Customer Managed AWS KMS keys

- [CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili
- [CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato
- [CodeBuild.3] I log CodeBuild S3 devono essere crittografati
- [CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]
- [CodeBuild.7] le esportazioni dei gruppi di CodeBuild report devono essere crittografate quando sono inattive
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [DataSync.1] DataSync le attività dovrebbero avere la registrazione abilitata
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata

- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup
- [DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup

- [EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate
- [EC2.40] I gateway NAT EC2 devono essere etichettati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto
- [EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server
- [EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR
- [EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry
- [EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2
- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag
- [ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ECR.5] I repository ECR devono essere crittografati e gestiti dal cliente AWS KMS keys

- [ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host
- [ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati
- [ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root
- [ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore
- [ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione
- [ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate
- [ECS.12] I cluster ECS devono utilizzare Container Insights
- [ECS.16] I set di attività ECS non devono assegnare automaticamente indirizzi IP pubblici
- [ECS.17] Le definizioni delle attività ECS non devono utilizzare la modalità di rete host
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio
- [EFS.7] I file system EFS devono avere i backup automatici abilitati
- [EFS.8] I file system EFS devono essere crittografati quando sono inattivi
- [EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata
- [EKS.7] Le configurazioni dei provider di identità EKS devono essere contrassegnate
- [EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità
- [ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità

- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate

- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ
- [FSx.4] I file system FSx for NetApp ONTAP devono essere configurati per l'implementazione Multi-AZ
- [FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato
- [GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato
- [GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata
- [GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata
- [GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide

- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
- [IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
- [IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
- [IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
- [IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
- [IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
- [IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate

- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi
- [Kinesis.3] I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [KMS.5] Le chiavi KMS non devono essere accessibili al pubblico
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato

- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MQ.4] I broker Amazon MQ devono essere etichettati
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker
- [MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata

- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.26] Le istanze DB RDS devono essere protette da un piano di backup
- [RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.36] Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch

- [RDS.38] Le istanze DB RDS per PostgreSQL devono essere crittografate in transito
- [RDS.39] Le istanze DB RDS per MySQL devono essere crittografate in transito
- [RDS.40] Le istanze DB di RDS per SQL Server devono pubblicare i log in Logs CloudWatch
- [RDS.41] Le istanze DB di RDS per SQL Server devono essere crittografate in transito
- [RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch
- [] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43
- [RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [RDS.46] Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso gateway Internet
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata
- [Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate
- [Redshift.16] I gruppi di sottoreti del cluster Redshift devono avere sottoreti provenienti da più zone di disponibilità
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch

- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni
- [S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita
- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- [S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3
- [S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita
- [S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata
- [S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto
- [S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container

- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.4] I documenti SSM non devono essere pubblici
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata
- [Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint

- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Cina (Pechino)

I seguenti controlli non sono supportati nella regione Cina (Pechino).

- [ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato
- [ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.2] Le fasi API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend
- [APIGateway.10] Le integrazioni API Gateway V2 devono utilizzare HTTPS per le connessioni private
- [APIGateway.11] I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate
- [Amplify.1] Le app Amplify devono essere taggate

- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.2] Le politiche di pianificazione dei batch devono essere etichettate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato

- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudTrail.10] I data store di eventi di CloudTrail Lake devono essere crittografati con Customer Managed AWS KMS keys
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate
- [Cognito.4] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata
- [Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito
- [Cognito.6] I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata

- [DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [DataSync.2] le DataSync attività devono essere etichettate
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.20] Entrambi i tunnel VPN per un AWS Site-to-Site La connessione VPN dovrebbe essere attiva
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup
- [EC2.36] I gateway per i clienti EC2 devono essere etichettati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto

- [EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.174] I set di opzioni DHCP EC2 devono essere etichettati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2
- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.21] I gruppi target di Application e Network Load Balancer devono utilizzare protocolli di controllo dello stato crittografati
- [ELB.22] I gruppi target ELB devono utilizzare protocolli di trasporto crittografati
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch

- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo
- [EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [GuardDuty.3] Gli GuardDuty IPSets devono essere etichettati
- [GuardDuty.4] i GuardDuty rilevatori devono essere etichettati
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato
- [GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato
- [GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata
- [GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata
- [GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.9] L'MFA deve essere abilitata per l'utente root

- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.23] Gli analizzatori IAM Access Analyzer devono essere etichettati
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Macie.1] Amazon Macie dovrebbe essere abilitato

- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch

- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata
- [PCA.2] AWS Le autorità di certificazione CA private devono essere contrassegnate
- [RDS.7] I cluster RDS devono avere la protezione da eliminazione abilitata
- [RDS.12] L'autenticazione IAM deve essere configurata per i cluster RDS
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.15] I cluster RDS DB devono essere configurati per più zone di disponibilità
- [RDS.16] I cluster Aurora DB devono essere configurati per copiare i tag nelle istantanee DB
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.26] Le istanze DB RDS devono essere protette da un piano di backup
- [RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi
- [RDS.28] I cluster RDS DB devono essere etichettati
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch
- [RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch
- [] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43
- [RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata

- [RDS.47] I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.48] I cluster RDS per MySQL DB devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.50] I cluster RDS DB devono avere un periodo di conservazione dei backup sufficiente
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate
- [Redshift.17] I gruppi di parametri del cluster Redshift devono essere etichettati
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto
- [S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container

- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.1] Gli elenchi di contatti SES devono essere etichettati
- [SES.2] I set di configurazione SES devono essere etichettati
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SSM.5] I documenti SSM devono essere etichettati
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [Transfer.5] I certificati Transfer Family devono essere etichettati
- [Transfer.6] I connettori Transfer Family devono essere etichettati
- [Transfer.7] I profili Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola

- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Cina (Ningxia)

I seguenti controlli non sono supportati nella regione Cina (Ningxia).

- [ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato
- [ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.2] Le fasi API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend
- [APIGateway.10] Le integrazioni API Gateway V2 devono utilizzare HTTPS per le connessioni private
- [APIGateway.11] I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi

- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.2] Le politiche di pianificazione dei batch devono essere etichettate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine

- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudTrail.10] I data store di eventi di CloudTrail Lake devono essere crittografati con Customer Managed AWS KMS keys
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate
- [Cognito.4] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata
- [Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito
- [Cognito.6] I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [DataSync.2] le DataSync attività devono essere etichettate
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato

- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.20] Entrambi i tunnel VPN per un AWS Site-to-Site La connessione VPN dovrebbe essere attiva
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup
- [EC2.36] I gateway per i clienti EC2 devono essere etichettati
- [EC2.50] I gateway VPN EC2 devono essere etichettati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.174] I set di opzioni DHCP EC2 devono essere etichettati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2

- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.21] I gruppi target di Application e Network Load Balancer devono utilizzare protocolli di controllo dello stato crittografati
- [ELB.22] I gruppi target ELB devono utilizzare protocolli di trasporto crittografati
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo
- [EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione

- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate
- [GuardDuty.3] Gli GuardDuty IPSets devono essere etichettati
- [GuardDuty.4] i GuardDuty rilevatori devono essere etichettati
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato
- [GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato
- [GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata
- [GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata
- [GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.23] Gli analizzatori IAM Access Analyzer devono essere etichettati
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati

- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Lambda.1] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico
- [Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati
- [Lambda.3] Le funzioni Lambda devono trovarsi in un VPC
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Lambda.6] Le funzioni Lambda devono essere etichettate
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata

- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata
- [PCA.2] AWS Le autorità di certificazione CA private devono essere contrassegnate
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.26] Le istanze DB RDS devono essere protette da un piano di backup
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch

- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch
- [] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43
- [RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [RDS.50] I cluster RDS DB devono avere un periodo di conservazione dei backup sufficiente
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate
- [Redshift.17] I gruppi di parametri del cluster Redshift devono essere etichettati
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container

- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SSM.5] I documenti SSM devono essere etichettati
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [StepFunctions.2] Le attività di Step Functions devono essere etichettate
- [Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [Transfer.5] I certificati Transfer Family devono essere etichettati
- [Transfer.6] I connettori Transfer Family devono essere etichettati
- [Transfer.7] I profili Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione

- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Europa (Francoforte)

I seguenti controlli non sono supportati nella regione Europa (Francoforte).

- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati

- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Europa (Irlanda)

I seguenti controlli non sono supportati nella regione Europa (Irlanda).

- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate

- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Europa (Londra)

I seguenti controlli non sono supportati nella regione Europa (Londra).

- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato

- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati

- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

Europa (Milano)

I seguenti controlli non sono supportati nella regione Europa (Milano).

- [APIGateway.11] I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata

- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati

- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito

- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [RDS.1] L'istantanea RDS deve essere privata
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita

- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SSM.2] Le istanze Amazon EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità delle patch pari a COMPLIANT dopo l'installazione della patch
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Europa (Parigi)

I seguenti controlli non sono supportati nella regione Europa (Parigi).

- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato

- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate

- [FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione

- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Europa (Spagna)

I seguenti controlli non sono supportati nella regione Europa (Spagna).

- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica

- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate

- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi

- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.1] Le istantanee di Amazon EBS non devono essere configurate per essere ripristinabili pubblicamente
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate
- [EC2.40] I gateway NAT EC2 devono essere etichettati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager

- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere

- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate

- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [Lambda.1] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MQ.4] I broker Amazon MQ devono essere etichettati
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata

- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [RDS.1] L'istantanea RDS deve essere privata
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook

- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.1] Gli elenchi di contatti SES devono essere etichettati
- [SES.2] I set di configurazione SES devono essere etichettati
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola

- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Europa (Stoccolma)

I seguenti controlli non sono supportati nella regione Europa (Stoccolma).

- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata

- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati

- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola

- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Europa (Zurigo)

I seguenti controlli non sono supportati nella regione Europa (Zurigo).

- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata

- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico
- [CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard

- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito

- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito

- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM

- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati

- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MQ.4] I broker Amazon MQ devono essere etichettati
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch

- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [RDS.1] L'istantanea RDS deve essere privata
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container

- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole

- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Israele (Tel Aviv)

I seguenti controlli non sono supportati nella regione di Israele (Tel Aviv).

- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata
- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica

- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata

- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato

- [EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup
- [EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate
- [EC2.40] I gateway NAT EC2 devono essere etichettati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR
- [EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry
- [EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag
- [ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati

- [ECR.5] I repository ECR devono essere crittografati e gestiti dal cliente AWS KMS keys
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EFS.8] I file system EFS devono essere crittografati quando sono inattivi
- [EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata
- [EKS.7] Le configurazioni dei provider di identità EKS devono essere contrassegnate
- [EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata
- [ELB.2] I sistemi Classic Load Balancer con SSL/HTTPS listener devono utilizzare un certificato fornito da AWS Certificate Manager
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati

- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
- [IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
- [IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
- [IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
- [IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
- [IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password

- [IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati

- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi
- [Kinesis.3] I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MQ.4] I broker Amazon MQ devono essere etichettati
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker
- [MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche

- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [RDS.1] L'istantanea RDS deve essere privata
- [RDS.4] Gli snapshot del cluster RDS e gli snapshot del database devono essere crittografati quando sono inattivi
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.26] Le istanze DB RDS devono essere protette da un piano di backup
- [RDS.29] Gli snapshot del cluster RDS DB devono essere etichettati
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch
- [Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ

- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore

- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.4] I documenti SSM non devono essere pubblici
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Messico (centrale)

I seguenti controlli non sono supportati nella regione Messico (Centrale).

- [ACM.1] ACM-issued I certificati importati devono essere rinnovati dopo un periodo di tempo specificato
- [ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- [Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione

- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [APIGateway.10] Le integrazioni API Gateway V2 devono utilizzare HTTPS per le connessioni private
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata
- [AppSync.4] AWS AppSync Le API GraphQL devono essere etichettate
- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [Athena.4] I gruppi di lavoro Athena dovrebbero avere la registrazione abilitata
- [AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità
- [AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)
- [AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità
- [AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [Backup.2] AWS Backup i punti di ripristino devono essere etichettati
- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.2] Le politiche di pianificazione dei batch devono essere etichettate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati

- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata

- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico
- [CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
- [CloudTrail.10] I data store di eventi di CloudTrail Lake devono essere crittografati con Customer Managed AWS KMS keys
- [CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili
- [CodeBuild.2] le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato
- [CodeBuild.3] I log CodeBuild S3 devono essere crittografati
- [CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]
- [CodeBuild.7] le esportazioni dei gruppi di CodeBuild report devono essere crittografate quando sono inattive
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate
- [Cognito.4] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata
- [Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito

- [Cognito.6] I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [DataSync.1] DataSync le attività dovrebbero avere la registrazione abilitata
- [DataSync.2] le DataSync attività devono essere etichettate
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch

- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup
- [DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup
- [EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere contrassegnate
- [EC2.40] I gateway NAT EC2 devono essere etichettati
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto
- [EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server
- [EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR
- [EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry
- [EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts

- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata
- [EC2.172] Le impostazioni VPC Block Public Access di EC2 dovrebbero bloccare il traffico del gateway Internet
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.174] I set di opzioni DHCP EC2 devono essere etichettati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.182] Le impostazioni di blocco dell'accesso pubblico devono essere abilitate per gli snapshot di Amazon EBS
- [EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2
- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag
- [ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ECR.5] I repository ECR devono essere crittografati e gestiti dal cliente AWS KMS keys
- [ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host
- [ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati
- [ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root
- [ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore

- [ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione
- [ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate
- [ECS.12] I cluster ECS devono utilizzare Container Insights
- [ECS.16] I set di attività ECS non devono assegnare automaticamente indirizzi IP pubblici
- [ECS.17] Le definizioni delle attività ECS non devono utilizzare la modalità di rete host
- [ECS.18] Le definizioni delle attività ECS devono utilizzare la crittografia in transito per i volumi EFS
- [ECS.19] I provider di capacità ECS dovrebbero avere abilitato la protezione gestita dalle terminazioni
- [ECS.20] Le definizioni delle attività ECS devono configurare gli utenti non root nelle definizioni dei container Linux
- [ECS.21] Le definizioni delle attività ECS devono configurare gli utenti non amministratori nelle definizioni dei contenitori Windows
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio
- [EFS.7] I file system EFS devono avere i backup automatici abilitati
- [EFS.8] I file system EFS devono essere crittografati quando sono inattivi
- [EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata
- [EKS.7] Le configurazioni dei provider di identità EKS devono essere contrassegnate
- [EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata
- [EKS.9] I gruppi di nodi EKS devono essere eseguiti su una versione di Kubernetes supportata
- [ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità
- [ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità

- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo
- [EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito
- [ES.3] I domini Elasticsearch devono crittografare i dati inviati tra i nodi
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [ES.9] I domini Elasticsearch devono essere etichettati
- [EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata

- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ
- [FSx.4] I file system FSx for NetApp ONTAP devono essere configurati per l'implementazione Multi-AZ
- [FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.1] AWS Glue i lavori devono essere etichettati
- [Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.1] GuardDuty dovrebbe essere abilitato
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato
- [GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato
- [GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata
- [GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata
- [GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi

- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.7] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.10] Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide
- [IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
- [IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
- [IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
- [IAM.14] Assicurati che la policy sulle password di IAM richieda almeno un numero
- [IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
- [IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
- [IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato

- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoT.4]AWS IoT Coregli autorizzatori devono essere etichettati
- [IoT.5]AWS IoT Coregli alias di ruolo devono essere etichettati
- [IoT.6]AWS IoT Corele politiche devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi
- [Kinesis.3] I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato

- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [KMS.5] Le chiavi KMS non devono essere accessibili al pubblico
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [MQ.4] I broker Amazon MQ devono essere etichettati
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker
- [MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità

- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata
- [PCA.2] AWS Le autorità di certificazione CA private devono essere contrassegnate
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato

- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.26] Le istanze DB RDS devono essere protette da un piano di backup
- [RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.36] Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch
- [RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch
- [RDS.38] Le istanze DB RDS per PostgreSQL devono essere crittografate in transito
- [RDS.39] Le istanze DB RDS per MySQL devono essere crittografate in transito
- [RDS.40] Le istanze DB di RDS per SQL Server devono pubblicare i log in Logs CloudWatch
- [RDS.41] Le istanze DB di RDS per SQL Server devono essere crittografate in transito
- [RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch
- [] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43
- [RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [RDS.46] Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso gateway Internet
- [RDS.47] I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.48] I cluster RDS per MySQL DB devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata
- [Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico
- [Redshift.2] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito
- [Redshift.3] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate
- [Redshift.4] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata
- [Redshift.6] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati

- [Redshift.7] I cluster Redshift devono utilizzare un routing VPC avanzato
- [Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.11] I cluster Redshift devono essere etichettati
- [Redshift.13] Le istantanee del cluster Redshift devono essere etichettate
- [Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate
- [Redshift.16] I gruppi di sottoreti del cluster Redshift devono avere sottoreti provenienti da più zone di disponibilità
- [Redshift.17] I gruppi di parametri del cluster Redshift devono essere etichettati
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni
- [S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita
- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- [S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3

- [S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita
- [S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata
- [S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto
- [S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato

- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.1] Gli elenchi di contatti SES devono essere etichettati
- [SES.2] I set di configurazione SES devono essere etichettati
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione
- [SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT
- [SSM.4] I documenti SSM non devono essere pubblici
- [SSM.5] I documenti SSM devono essere etichettati
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata
- [Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati

- [Transfer.5] I certificati Transfer Family devono essere etichettati
- [Transfer.6] I connettori Transfer Family devono essere etichettati
- [Transfer.7] I profili Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Medio Oriente (Bahrein)

I seguenti controlli non sono supportati nella regione Medio Oriente (Bahrein).

- [APIGateway.11] I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys

- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudTrail.10] I data store di eventi di CloudTrail Lake devono essere crittografati con Customer Managed AWS KMS keys
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate

- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DocumentDB.6] I cluster Amazon DocumentDB devono essere crittografati in transito
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.20] Entrambi i tunnel VPN per un AWS Site-to-Site La connessione VPN dovrebbe essere attiva
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ECR.5] I repository ECR devono essere crittografati e gestiti dal cliente AWS KMS keys
- [ECS.17] Le definizioni delle attività ECS non devono utilizzare la modalità di rete host
- [EKS.9] I gruppi di nodi EKS devono essere eseguiti su una versione di Kubernetes supportata
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate

- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ
- [FSx.4] I file system FSx for NetApp ONTAP devono essere configurati per l'implementazione Multi-AZ
- [FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate

- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [NetworkFirewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RDS.41] Le istanze DB di RDS per SQL Server devono essere crittografate in transito
- [RDS.42] Le istanze RDS per MariaDB DB dovrebbero pubblicare i log su Logs CloudWatch
- [] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43
- [RDS.44] Le istanze RDS per MariaDB DB devono essere crittografate in transito
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [RDS.46] Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso gateway Internet
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.4] I namespace Serverless di Redshift devono essere crittografati con gestione del cliente AWS KMS keys
- [RedshiftServerless.5] I namespace Redshift Serverless non devono utilizzare il nome utente amministratore predefinito
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati

- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.8] le istanze SageMaker notebook devono essere eseguite su piattaforme supportate
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Medio Oriente (Emirati Arabi Uniti)

I seguenti controlli non sono supportati nella regione del Medio Oriente (Emirati Arabi Uniti).

- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [APIGateway.11] I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate
- [Amplify.1] Le app Amplify devono essere taggate

- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi
- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFormation.3] gli CloudFormation stack dovrebbero avere la protezione dalla terminazione abilitata
- [CloudFormation.4] gli CloudFormation stack devono avere ruoli di servizio associati
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS

- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [Detective.1] I grafici del comportamento dei Detective devono essere etichettati
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate
- [DMS.4] Le istanze di replica DMS devono essere etichettate
- [DMS.5] I sottoreti di replica DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato

- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato
- [DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato
- [DMS.13] Le istanze di replica DMS devono essere configurate per utilizzare più zone di disponibilità
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.4] Le istanze EC2 interrotte devono essere rimosse dopo un periodo di tempo specificato
- [EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0. 0/0 oppure: :/0 alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati

- [EC2.180] Le interfacce di rete EC2 dovrebbero avere il controllo abilitato source/destination
- [EC2.181] I modelli di lancio EC2 dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.183] Le connessioni VPN EC2 devono utilizzare il protocollo IKEv2
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS
- [EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup
- [EKS.9] I gruppi di nodi EKS devono essere eseguiti su una versione di Kubernetes supportata
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate
- [ELB.18] I listener di Application e Network Load Balancer devono utilizzare protocolli sicuri per crittografare i dati in transito
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata

- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue
- [GuardDuty.2] GuardDuty i filtri devono essere etichettati
- [IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
- [IAM.2] Gli utenti IAM non devono avere policy IAM allegate
- [IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
- [IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
- [IAM.5] L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con Supporto AWS
- [IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata
- [Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata
- [Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata

- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [KMS.1] Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS
- [KMS.2] I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- [Lambda.7] Le funzioni Lambda dovrebbero avere AWS X-Ray tracciamento attivo abilitato
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.4] L'accesso pubblico ai cluster MSK dovrebbe essere disabilitato
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [MSK.6] I cluster MSK devono disabilitare l'accesso non autenticato
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico

- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [Opensearch.9] i OpenSearch domini devono essere etichettati
- [Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software
- [Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata
- [Redshift.18] I cluster Redshift dovrebbero avere le implementazioni abilitate Multi-AZ
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato

- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari
- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.1] Gli elenchi di contatti SES devono essere etichettati
- [SES.2] I set di configurazione SES devono essere etichettati
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive
- [] Le code SQS devono essere etichettate SQS.2
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch

- [SSM.7] I documenti SSM devono avere l'impostazione di condivisione pubblica a blocchi abilitata
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

Sud America (San Paolo)

I seguenti controlli non sono supportati nella regione Sud America (San Paolo).

- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato

- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato
- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati

- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoT.1]AWS IoT Device Defenderi profili di sicurezza devono essere etichettati
- [IoT.2]AWS IoT Corele azioni di mitigazione devono essere etichettate
- [IoT.3]AWS IoT Corele dimensioni devono essere etichettate
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione

- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole

AWS GovCloud (US-East)

I seguenti controlli non sono supportati nella AWS GovCloud (US-East) regione.

- [ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- [Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.2] Le fasi API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [APIGateway.10] Le integrazioni API Gateway V2 devono utilizzare HTTPS per le connessioni private
- [APIGateway.11] I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata
- [AppSync.4] AWS AppSync Le API GraphQL devono essere etichettate

- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità
- [AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)
- [AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità
- [AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2
- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.2] Le politiche di pianificazione dei batch devono essere etichettate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato

- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeBuild.3] I log CodeBuild S3 devono essere crittografati
- [CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.2] I pool di identità di Cognito non dovrebbero consentire identità non autenticate
- [Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate
- [Cognito.4] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata
- [Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito
- [Cognito.6] I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata

- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati
- [Connect.2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata
- [DataSync.2] le DataSync attività devono essere etichettate
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.47] I servizi endpoint Amazon VPC devono essere etichettati
- [EC2.52] I gateway di transito EC2 devono essere etichettati

- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts
- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.174] I set di opzioni DHCP EC2 devono essere etichettati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag
- [ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host
- [ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati
- [ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root
- [ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore
- [ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione
- [ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate
- [ECS.12] I cluster ECS devono utilizzare Container Insights
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata
- [EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata

- [ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità
- [ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.21] I gruppi target di Application e Network Load Balancer devono utilizzare protocolli di controllo dello stato crittografati
- [ELB.22] I gruppi target ELB devono utilizzare protocolli di trasporto crittografati
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo
- [EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata

- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata
- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato
- [GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata
- [GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati

- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate
- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi
- [KMS.5] Le chiavi KMS non devono essere accessibili al pubblico
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker
- [MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati

- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata
- [PCA.2] AWS Le autorità di certificazione CA private devono essere contrassegnate
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.15] I cluster RDS DB devono essere configurati per più zone di disponibilità
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato

- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi
- [RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch
- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [RDS.47] I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.48] I cluster RDS per MySQL DB devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.50] I cluster RDS DB devono avere un periodo di conservazione dei backup sufficiente
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata
- [Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.17] I gruppi di parametri del cluster Redshift devono essere etichettati
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita

- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- [S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3
- [S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita
- [S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.16] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per i contenitori primari

- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SageMaker.19] SageMaker i modelli dovrebbero utilizzare il registro privato in VPC per pipeline di inferenza multi-contenitore
- [SES.1] Gli elenchi di contatti SES devono essere etichettati
- [SES.2] I set di configurazione SES devono essere etichettati
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico
- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.4] I documenti SSM non devono essere pubblici
- [SSM.5] I documenti SSM devono essere etichettati
- [SSM.6] SSM Automation dovrebbe avere la registrazione abilitata CloudWatch
- [StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata
- [StepFunctions.2] Le attività di Step Functions devono essere etichettate
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [Transfer.5] I certificati Transfer Family devono essere etichettati
- [Transfer.6] I connettori Transfer Family devono essere etichettati
- [Transfer.7] I profili Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole

- [WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch
- [WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi
- [WorkSpaces.2] i volumi WorkSpaces root devono essere crittografati quando sono inattivi

AWS GovCloud (US-West)

I seguenti controlli non sono supportati nella AWS GovCloud (US-West) regione.

- [ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- [Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS
- [Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione
- [APIGateway.2] Le fasi API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend
- [APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione
- [APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [APIGateway.10] Le integrazioni API Gateway V2 devono utilizzare HTTPS per le connessioni private
- [APIGateway.11] I nomi di dominio API Gateway devono utilizzare le politiche di sicurezza consigliate
- [Amplify.1] Le app Amplify devono essere taggate
- [Amplify.2] I rami Amplify devono essere etichettati
- [AppConfig.1]AWS AppConfigle applicazioni devono essere etichettate
- [AppConfig.2]AWS AppConfigi profili di configurazione devono essere etichettati
- [AppConfig.3]AWS AppConfiggli ambienti devono essere etichettati
- [AppConfig.4]AWS AppConfigle associazioni di estensioni devono essere etichettate
- [AppFlow.1] I AppFlow flussi Amazon devono essere etichettati
- [AppRunner.1] I servizi App Runner devono essere etichettati
- [AppRunner.2] I connettori VPC App Runner devono essere etichettati
- [AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata
- [AppSync.4] AWS AppSync Le API GraphQL devono essere etichettate

- [AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API
- [AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità
- [AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)
- [AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità
- [AutoScaling.9] I gruppi Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2
- [Backup.4] AWS Backup i piani di report devono essere etichettati
- [Batch.1] Le code di lavoro in batch devono essere contrassegnate
- [Batch.2] Le politiche di pianificazione dei batch devono essere etichettate
- [Batch.3] Gli ambienti di calcolo in batch devono essere etichettati
- [Batch.4] Le proprietà delle risorse di calcolo negli ambienti di calcolo Batch gestiti devono essere etichettate
- [BedrockAgentCore.1] I AgentCore runtime Bedrock devono essere configurati con la modalità di rete VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways dovrebbe richiedere l'autorizzazione per le richieste in entrata
- [BedrockAgentCore.3] Bedrock AgentCore Memory deve essere crittografata e gestita dal cliente AWS KMS keys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway deve essere crittografato con Customer Managed AWS KMS keys
- [BedrockAgentCore.5] I browser personalizzati AgentCore Bedrock non devono utilizzare la modalità di rete pubblica
- [BedrockAgentCore.6] I browser AgentCore personalizzati Bedrock devono avere la registrazione delle sessioni abilitata
- [CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [CloudFront.4] le CloudFront distribuzioni dovrebbero avere il failover di origine configurato
- [CloudFront.5] CloudFront le distribuzioni dovrebbero avere la registrazione abilitata
- [CloudFront.6] le CloudFront distribuzioni devono avere WAF abilitato

- [CloudFront.7] CloudFront le distribuzioni devono utilizzare certificati personalizzati SSL/TLS
- [CloudFront.8] CloudFront le distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [CloudFront.9] CloudFront le distribuzioni devono crittografare il traffico verso origini personalizzate
- [CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [CloudFront.14] CloudFront le distribuzioni devono essere etichettate
- [CloudFront.15] CloudFront le distribuzioni devono utilizzare la politica di sicurezza TLS consigliata
- [CloudFront.16] CloudFront le distribuzioni dovrebbero utilizzare il controllo dell'accesso all'origine per le origini degli URL della funzione Lambda
- [CloudFront.17] CloudFront le distribuzioni devono utilizzare gruppi di chiavi affidabili per URL e cookie firmati
- [CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate
- [CodeArtifact.1] i CodeArtifact repository devono essere etichettati
- [CodeBuild.3] I log CodeBuild S3 devono essere crittografati
- [CodeBuild.4] gli ambienti di CodeBuild progetto dovrebbero avere una registrazione AWS Config[durata]
- [CodeGuruProfiler.1] I gruppi CodeGuru di profilazione Profiler devono essere etichettati
- [CodeGuruReviewer.1] Le associazioni CodeGuru dei repository dei revisori devono essere etichettate
- [Cognito.1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard
- [Cognito.3] Le politiche relative alle password per i pool di utenti di Cognito devono avere configurazioni avanzate
- [Cognito.4] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione personalizzata
- [Cognito.5] L'MFA deve essere abilitata per i pool di utenti di Cognito
- [Cognito.6] I pool di utenti di Cognito devono avere la protezione dall'eliminazione abilitata
- [Connect.1] I tipi di oggetto Amazon Connect Customer Profiles devono essere etichettati

- [DataSync.2] le DataSync attività devono essere etichettate
- [DMS.2] I certificati DMS devono essere etichettati
- [DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato
- [DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata
- [DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata
- [DMS.9] Gli endpoint DMS devono utilizzare SSL
- [DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi
- [DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato
- [DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- [DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch
- [DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata
- [DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito
- [EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso a partire dalla versione 0.0.0. 0/0 alla porta 22 o alla porta 3389
- [EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi
- [EC2.23] I gateway di transito Amazon EC2 non dovrebbero accettare automaticamente richieste di allegati VPC
- [EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete
- [EC2.28] I volumi EBS devono essere coperti da un piano di backup
- [EC2.38] Le istanze EC2 devono essere etichettate
- [EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts

- [EC2.60] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager
- [EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)
- [EC2.173] Le richieste EC2 Spot Fleet con parametri di avvio dovrebbero abilitare la crittografia per i volumi EBS collegati
- [EC2.174] I set di opzioni DHCP EC2 devono essere etichettati
- [EC2.175] I modelli di lancio di EC2 devono essere etichettati
- [EC2.176] Gli elenchi di prefissi EC2 devono essere etichettati
- [EC2.177] Le sessioni Traffic Mirror di EC2 devono essere etichettate
- [EC2.178] I filtri Traffic Mirror EC2 devono essere etichettati
- [EC2.179] Gli obiettivi del traffic mirror di EC2 devono essere etichettati
- [ECR.1] I repository privati ECR dovrebbero avere la scansione delle immagini configurata
- [ECR.2] I repository privati ECR devono avere configurata l'immutabilità dei tag
- [ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata
- [ECR.4] Gli archivi pubblici ECR devono essere etichettati
- [ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host
- [ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati
- [ECS.5] Le definizioni delle attività ECS devono configurare i contenitori in modo che siano limitati all'accesso in sola lettura ai filesystem root
- [ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore
- [ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione
- [ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate
- [ECS.12] I cluster ECS devono utilizzare Container Insights
- [EFS.3] I punti di accesso EFS devono applicare una directory principale
- [EFS.4] I punti di accesso EFS devono applicare un'identità utente
- [EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata
- [EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata
- [ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità

- [ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità
- [ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa
- [ELB.21] I gruppi target di Application e Network Load Balancer devono utilizzare protocolli di controllo dello stato crittografati
- [ELB.22] I gruppi target ELB devono utilizzare protocolli di trasporto crittografati
- I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati
- [ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati
- [ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- [ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi
- [ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito
- [ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato
- [ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito
- [ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata
- [ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati
- [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch
- [EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
- [EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo
- [EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito
- [ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch
- [EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata
- [EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata

- [FraudDetector.1] I tipi di entità Amazon Fraud Detector devono essere etichettati
- [FraudDetector.2] Le etichette di Amazon Fraud Detector devono essere etichettate
- [FraudDetector.3] I risultati di Amazon Fraud Detector devono essere etichettati
- [FraudDetector.4] Le variabili di Amazon Fraud Detector devono essere etichettate
- [FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi
- [FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato
- [GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata
- [GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata
- [GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato
- [GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato
- [GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato
- [IAM.6] La MFA hardware deve essere abilitata per l'utente root
- [IAM.9] L'MFA deve essere abilitata per l'utente root
- [IAM.21] Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi
- [IAM.24] I ruoli IAM devono essere etichettati
- [IAM.25] Gli utenti IAM devono essere etichettati
- [IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato
- [Inspector.3] La scansione del codice Amazon Inspector Lambda deve essere abilitata
- [IoTSiteWise.1]AWSI modelli di SiteWise asset IoT devono essere etichettati
- [IoTSiteWise.2]AWSI SiteWise dashboard IoT devono essere etichettati
- [IoTSiteWise.3]AWS SiteWise I gateway IoT devono essere etichettati
- [IoTSiteWise.4]AWS SiteWise I portali IoT devono essere etichettati
- [IoTSiteWise.5]AWS SiteWise I progetti IoT devono essere etichettati
- [IoTTwinMaker.1] AWS I lavori di TwinMaker sincronizzazione IoT devono essere etichettati
- [IoTTwinMaker.2] AWS TwinMaker Gli spazi di lavoro IoT devono essere etichettati
- [IoTTwinMaker.3] AWS TwinMaker Le scene IoT devono essere etichettate

- [IoTTwinMaker.4] AWS TwinMaker Le entità IoT devono essere etichettate
- [IoTWireless.1]AWSI gruppi multicast IoT Wireless devono essere etichettati
- [IoTWireless.2]AWSI profili dei servizi IoT Wireless devono essere etichettati
- [IoTWireless.3]AWSLe attività IoT FUOTA devono essere etichettate
- [IVS.1] Le coppie di tasti di riproduzione IVS devono essere etichettate
- [IVS.2] Le configurazioni di registrazione IVS devono essere etichettate
- [IVS.3] I canali IVS devono essere etichettati
- [Keyspaces.1] Gli spazi chiave di Amazon Keyspaces devono essere etichettati
- [Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi
- [KMS.5] Le chiavi KMS non devono essere accessibili al pubblico
- [Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità
- [Macie.1] Amazon Macie dovrebbe essere abilitato
- [Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato
- [MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby
- [MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster
- [MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker
- [MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato
- [MSK.3] I connettori MSK Connect devono essere crittografati in transito
- [MSK.5] I connettori MSK devono avere la registrazione abilitata
- [Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi
- [Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [Neptune.4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata
- [Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive
- [Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata
- [Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità

- [NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità
- [NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata
- [NetworkFirewall.3] Le politiche del Network Firewall devono avere almeno un gruppo di regole associato
- [NetworkFirewall.4] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [NetworkFirewall.5] L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [NetworkFirewall.6] Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [Opensearch.1] OpenSearch i domini devono avere la crittografia a riposo abilitata
- [Opensearch.2] i OpenSearch domini non devono essere accessibili al pubblico
- [Opensearch.3] i OpenSearch domini devono crittografare i dati inviati tra i nodi
- [Opensearch.4] la registrazione degli errori di OpenSearch dominio nei registri dovrebbe essere abilitata CloudWatch
- [Opensearch.5] i OpenSearch domini devono avere la registrazione di controllo abilitata
- [Opensearch.6] i OpenSearch domini devono avere almeno tre nodi di dati
- [Opensearch.7] i OpenSearch domini devono avere un controllo granulare degli accessi abilitato
- [Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente
- [PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata
- [PCA.2] AWS Le autorità di certificazione CA private devono essere contrassegnate
- [RDS.14] I cluster Amazon Aurora dovrebbero avere il backtracking abilitato
- [RDS.15] I cluster RDS DB devono essere configurati per più zone di disponibilità
- [RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato
- [RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi
- [RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch

- [] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato
- [] I proxy RDS DB devono richiedere la crittografia TLS per le connessioni RDS.43
- [RDS.45] I cluster Aurora MySQL DB devono avere la registrazione di controllo abilitata
- [RDS.47] I cluster DB RDS per PostgreSQL devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.48] I cluster RDS per MySQL DB devono essere configurati per copiare i tag nelle istantanee del DB
- [RDS.50] I cluster RDS DB devono avere un periodo di conservazione dei backup sufficiente
- [RDS.51] I cluster globali RDS devono essere eseguiti su una versione Aurora MySQL supportata
- [Redshift.7] I cluster Redshift devono utilizzare un routing VPC avanzato
- [Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito
- [Redshift.10] I cluster Redshift devono essere crittografati a riposo
- [Redshift.11] I cluster Redshift devono essere etichettati
- [Redshift.13] Le istantanee del cluster Redshift devono essere etichettate
- [Redshift.17] I gruppi di parametri del cluster Redshift devono essere etichettati
- [RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato
- [RedshiftServerless.2] Le connessioni ai gruppi di lavoro Serverless di Redshift devono essere necessarie per utilizzare SSL
- [RedshiftServerless.3] I gruppi di lavoro Serverless di Redshift dovrebbero vietare l'accesso pubblico
- [RedshiftServerless.6] I namespace Redshift Serverless dovrebbero esportare i log in Logs CloudWatch
- [Route53.1] I controlli sanitari della Route 53 devono essere etichettati
- [Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [S3.10] I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita
- [] I bucket S3 per uso generico devono S3.11 avere le notifiche degli eventi abilitate
- [S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3

- [S3.13] I bucket S3 per uso generico devono avere configurazioni del ciclo di vita
- [S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata
- [S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco dell'accesso pubblico abilitate
- [S3.25] I bucket di directory S3 devono avere configurazioni del ciclo di vita
- [SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato
- [SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.6] le configurazioni delle immagini delle SageMaker app devono essere contrassegnate
- [SageMaker.7] SageMaker le immagini devono essere taggate
- [SageMaker.9] le definizioni dei lavori SageMaker relativi alla qualità dei dati devono avere abilitata la crittografia del traffico tra container
- [SageMaker.10] le definizioni dei processi di spiegabilità dei SageMaker modelli devono avere abilitata la crittografia del traffico tra container
- [SageMaker.11] le definizioni dei processi di qualità SageMaker dei dati devono avere l'isolamento della rete abilitato
- [SageMaker.12] le definizioni dei job di SageMaker model bias devono avere l'isolamento della rete abilitato
- [SageMaker.13] le definizioni dei processi di qualità SageMaker del modello dovrebbero avere la crittografia del traffico tra container abilitata
- [SageMaker.14] le pianificazioni di SageMaker monitoraggio dovrebbero avere l'isolamento della rete abilitato
- [SageMaker.15] Le definizioni dei job di SageMaker model bias devono avere abilitata la crittografia del traffico tra container
- [SageMaker.17] i negozi offline del gruppo di SageMaker funzionalità devono essere crittografati con AWS KMS keys
- [SageMaker.18] I negozi online del gruppo di SageMaker funzionalità con archiviazione standard devono essere crittografati con AWS KMS keys
- [SES.3] I set di configurazione SES devono avere TLS abilitato per l'invio di e-mail
- [SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico

- [SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico
- [SSM.4] I documenti SSM non devono essere pubblici
- [SSM.5] I documenti SSM devono essere etichettati
- [StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata
- [StepFunctions.2] Le attività di Step Functions devono essere etichettate
- [Transfer.4] Gli accordi Transfer Family devono essere etichettati
- [Transfer.5] I certificati Transfer Family devono essere etichettati
- [Transfer.6] I connettori Transfer Family devono essere etichettati
- [Transfer.7] I profili Transfer Family devono essere etichettati
- [WAF.1] AWS WAF La registrazione classica Global Web ACL deve essere abilitata
- [WAF.2] AWS WAF Le regole regionali classiche devono avere almeno una condizione
- [WAF.3] AWS WAF I gruppi di regole regionali classici devono avere almeno una regola
- [WAF.4] AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole
- [WAF.6] AWS WAF Le regole globali classiche devono avere almeno una condizione
- [WAF.7] AWS WAF I gruppi di regole globali classici devono avere almeno una regola
- [WAF.8] AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole
- [WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole
- [WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch

Creazione di risorse CSPM Security Hub con CloudFormation

AWSSecurity Hub CSPM si integra conAWS CloudFormation, un servizio che consente di modellare e configurare le AWS risorse in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri (come le regole di automazione) e fornisce e configura CloudFormation tali risorse per te.

Quando lo utilizziCloudFormation, puoi riutilizzare il modello per configurare le risorse CSPM di Security Hub in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi fornisci le stesse risorse più e più volte in più Account AWS regioni.

Security Hub CSPM eCloudFormationmodelli

Per fornire e configurare le risorse per Security Hub CSPM e i servizi correlati, è necessario comprendere come funzionano i CloudFormationmodelli. I modelli sono file di testo in formato JSON o YAML. Questi modelli descrivono le risorse che desideri inserire negli stack. CloudFormation

Se non conosci JSON o YAML, puoi usare CloudFormation Designer per iniziare a usare i modelli. CloudFormation Per ulteriori informazioni, consulta Cos'è Designer? CloudFormation nella Guida AWS CloudFormation per l'utente.

È possibile creare CloudFormation modelli per i seguenti tipi di risorse CSPM di Security Hub:

- Abilitazione del Security Hub CSPM
- Designazione dell'amministratore CSPM delegato del Security Hub per un'organizzazione
- Specificate il modo in cui la vostra organizzazione è configurata in Security Hub CSPM
- Abilitazione di uno standard di sicurezza
- Abilitazione dell'aggregazione tra regioni
- Creazione di una politica di configurazione centrale e associazione agli account, alle unità organizzative (OU) o alla radice
- Creazione di informazioni dettagliate personalizzate
- Creazione di una regola di automazione
- Personalizzazione dei parametri di controllo
- Abbonamento a un'integrazione di prodotti di terze parti

Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per le risorse, consultate il riferimento al tipo di risorsa AWS Security Hub CSPM nella Guida per l'utente. AWS CloudFormation

Scopri di più suCloudFormation

Per ulteriori informazioniCloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormationGuida per l'utente
- CloudFormationDocumentazione di riferimento delle API
- AWS CloudFormationGuida per l'utente dell'interfaccia a riga di comando

Iscrizione agli annunci CSPM di Security Hub con Amazon SNS

Questa sezione fornisce informazioni sulla sottoscrizione agli annunci CSPM AWS di Security Hub con Amazon Simple Notification Service (Amazon SNS) per ricevere notifiche su Security Hub CSPM.

Dopo l'iscrizione, riceverai notifiche sui seguenti eventi (nota il corrispondente per ogni evento): `AnnouncementType`

- `NEW_STANDARDS_CONTROLS`— Sono stati aggiunti nuovi controlli o standard CSPM di Security Hub.
- `RETIRED_STANDARDS_CONTROLS`— I controlli o gli standard CSPM esistenti di Security Hub sono stati ritirati.

Le notifiche sono disponibili in tutti i formati supportati da Amazon SNS. Puoi iscriverti agli annunci CSPM di Security Hub in tutte le versioni in cui Security Regioni AWS Hub CSPM è disponibile.

Un utente deve disporre `Subscribe` delle autorizzazioni per iscriversi a un argomento di Amazon SNS. Puoi raggiungere questo obiettivo con le policy di Amazon SNS, le policy IAM o entrambe. Per ulteriori informazioni, consulta le politiche di IAM e Amazon SNS insieme nella Amazon Simple Notification Service Developer Guide.

> **Note**
>
> Security Hub CSPM invia annunci Amazon SNS sugli aggiornamenti del servizio CSPM di Security Hub a tutti gli abbonati. Account AWS Per ricevere notifiche sui risultati del CSPM di Security Hub, vedere. Revisione dei dettagli e della cronologia dei risultati in Security Hub CSPM

Puoi abbonarti a una coda Amazon Simple Queue Service (Amazon SQS) per un argomento Amazon SNS, ma devi utilizzare un argomento Amazon SNS Amazon Resource Name (ARN) che si trova nella stessa regione. Per ulteriori informazioni, consulta l'argomento Sottoscrizione di una coda a un Amazon SNS nella Amazon Simple Queue Service Developer Guide.

Puoi anche utilizzare una AWS Lambda funzione per richiamare eventi quando ricevi notifiche. Per ulteriori informazioni, incluso un codice di funzione di esempio, consulta Tutorial: Using AWS Lambda with Amazon Simple Notification Service nella AWS LambdaDeveloper Guide.

Gli ARN dell'argomento Amazon SNS per ogni regione sono i seguenti.

Regione AWS	ARN di un argomento Amazon SNS
Stati Uniti orientali (Ohio)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
Stati Uniti orientali (Virginia settentrionale)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
Stati Uniti occidentali (California settentrionale)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
Stati Uniti occidentali (Oregon)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`
Africa (Città del Capo)	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`
Asia Pacifico (Hong Kong)	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`
Asia Pacific (Hyderabad)	`arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements`
Asia Pacifico (Giacarta)	`arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements`
Asia Pacifico (Mumbai)	`arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements`

Regione AWS	ARN di un argomento Amazon SNS
Asia Pacifico (Osaka)	`arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements`
Asia Pacifico (Seoul)	`arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements`
Asia Pacifico (Singapore)	`arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements`
Asia Pacifico (Sydney)	`arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements`
Asia Pacifico (Tokyo)	`arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements`
Canada (Centrale)	`arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements`
Cina (Pechino)	`arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements`
Cina (Ningxia)	`arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements`
Europa (Francoforte)	`arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements`

Regione AWS	ARN di un argomento Amazon SNS
Europa (Irlanda)	`arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements`
Europa (Londra)	`arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements`
Europa (Milano)	`arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements`
Europa (Parigi)	`arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements`
Europa (Spagna)	`arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements`
Europa (Stoccolma)	`arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements`
Europa (Zurigo)	`arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements`
Israele (Tel Aviv)	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
Medio Oriente (Bahrein)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`

Regione AWS	ARN di un argomento Amazon SNS
Medio Oriente (Emirati Arabi Uniti)	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
Sud America (San Paolo)	`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`

I messaggi sono in genere gli stessi in tutte le regioni all'interno di una partizione, quindi puoi iscriverti a una regione in ogni partizione per ricevere annunci che riguardano tutte le regioni di quella partizione. Gli annunci associati agli account dei membri non vengono replicati nell'account amministratore. Di conseguenza, ogni account, incluso l'account amministratore, avrà solo una copia di ogni annuncio. Puoi decidere quale account utilizzare per iscriverti agli annunci CSPM di Security Hub.

Per informazioni sul costo dell'abbonamento agli annunci CSPM di Security Hub, consulta i prezzi di Amazon SNS.

Iscrizione agli annunci CSPM di Security Hub (console)

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nell'elenco delle regioni, scegli la regione in cui desideri iscriverti agli annunci CSPM di Security Hub. Questo esempio utilizza la regione `us-west-2`.
3. Nel riquadro di navigazione scegliere Subscriptions (Sottoscrizioni), quindi selezionare Create subscription (Crea sottoscrizione).
4. Inserisci l'argomento ARN nella casella Argomento ARN. Ad esempio, `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.

5. Per Protocollo, scegli come desideri ricevere gli annunci CSPM di Security Hub. Se scegli Email, for Endpoint, inserisci l'indirizzo email che desideri utilizzare per ricevere annunci.
6. Scegli Create Subscription (Crea sottoscrizione).
7. Confermare la sottoscrizione. Ad esempio, se hai scelto il protocollo e-mail, Amazon SNS invierà un messaggio di conferma dell'iscrizione all'indirizzo e-mail che hai fornito.

Iscrizione agli annunci CSPM di Security Hub (AWS CLI)

1. Esegui il comando seguente:

```
 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. Confermare la sottoscrizione. Ad esempio, se hai scelto il protocollo e-mail, Amazon SNS invierà un messaggio di conferma dell'iscrizione all'indirizzo e-mail che hai fornito.

Formato dei messaggi Amazon SNS

Gli esempi seguenti mostrano gli annunci CSPM di Security Hub di Amazon SNS sull'introduzione di nuovi controlli di sicurezza. Il contenuto dei messaggi varia in base al tipo di annuncio, ma il formato è lo stesso per tutti i tipi di annuncio. Facoltativamente, può essere incluso un `Link` campo che fornisce dettagli sull'annuncio.

Esempio: annuncio CSPM di Security Hub per nuovi controlli (protocollo e-mail)

```
{
"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. "
}
```

Esempio: annuncio CSPM di Security Hub per nuovi controlli (protocollo Email-JSON)

```
{
  "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"
}
```

Disattivazione del Security Hub CSPM

È possibile disabilitare AWS Security Hub CSPM utilizzando la console Security Hub CSPM o l'API Security Hub. Se disabiliti Security Hub CSPM, puoi riattivarlo in un secondo momento.

Se l'organizzazione utilizza la configurazione centrale, l'amministratore delegato di Security Hub CSPM può creare policy di configurazione che disabilitano Security Hub CSPM per account e unità organizzative (OU) specifici e mantengono abilitato Security Hub CSPM per altri. Le politiche di configurazione influiscono sulla regione di origine e su tutte le regioni collegate. Per ulteriori informazioni, consulta Comprendere la configurazione centrale in Security Hub CSPM.

Se si disabilita Security Hub CSPM per un account, si verifica quanto segue:

- Tutti gli standard e i controlli CSPM di Security Hub sono disabilitati per l'account.
- Security Hub CSPM interrompe la generazione, l'aggiornamento e l'acquisizione dei risultati per l'account.
- Dopo 30 giorni, Security Hub CSPM elimina definitivamente tutti i risultati archiviati esistenti per l'account. I risultati non possono essere recuperati utilizzando Security Hub CSPM.
- Dopo 90 giorni, Security Hub CSPM elimina definitivamente tutti i risultati attivi esistenti per l'account. I risultati non possono essere recuperati utilizzando Security Hub CSPM.
- Dopo 90 giorni, Security Hub CSPM elimina definitivamente tutti gli approfondimenti esistenti e le impostazioni di configurazione CSPM di Security Hub per l'account. I dati e le impostazioni non possono essere ripristinati.

Per conservare i risultati esistenti, puoi esportare i risultati in un bucket S3 prima di disabilitare Security Hub CSPM. Puoi farlo utilizzando un'azione personalizzata con una EventBridge regola Amazon. Per ulteriori informazioni, consulta Utilizzo EventBridge per la risposta e la correzione automatiche.

Se riattivi Security Hub CSPM entro 90 giorni dalla disattivazione per un account, riottieni l'accesso ai risultati attivi esistenti, nonché agli approfondimenti e alle impostazioni di configurazione CSPM di Security Hub per l'account. Se riattivi Security Hub CSPM entro 30 giorni, riottieni anche l'accesso

ai risultati archiviati esistenti per l'account. Tuttavia, i risultati esistenti potrebbero essere imprecisi perché rifletteranno lo stato dell'AWSambiente quando hai disabilitato Security Hub CSPM. Inoltre, quando riattivi singoli standard e controlli, Security Hub CSPM potrebbe inizialmente generare risultati duplicati per AWS risorse specifiche, a seconda degli standard e dei controlli abilitati. Per questi motivi, ti consigliamo di effettuare una delle seguenti operazioni:

- Modifica lo stato del flusso di lavoro di tutti i risultati esistenti impostandolo su `RESOLVED` prima di disabilitare Security Hub CSPM. Per ulteriori informazioni, consulta Impostazione dello stato dei risultati del flusso di lavoro.
- Disabilita tutti gli standard almeno sei giorni prima di disabilitare Security Hub CSPM. Security Hub CSPM archivia quindi tutti i risultati esistenti con il massimo impegno, in genere entro tre-cinque giorni. Per ulteriori informazioni, consulta Disabilitazione di uno standard.

Non puoi disabilitare Security Hub CSPM nei seguenti casi:

- Il tuo account è l'account amministratore CSPM di Security Hub delegato per un'organizzazione. Se si utilizza la configurazione centrale, non è possibile associare una politica di configurazione che disabiliti Security Hub CSPM per l'account amministratore delegato. L'associazione può avere successo per altri account, ma Security Hub CSPM non applica la politica all'account amministratore delegato.
- Il tuo account è un account amministratore CSPM di Security Hub su invito e disponi di account membri. Prima di poter disabilitare Security Hub CSPM, devi dissociare tutti i tuoi account membro. Per scoprire come, consulta the section called “Dissociazione degli account dei membri”.

Prima che il proprietario di un account membro possa disabilitare Security Hub CSPM, l'account deve dissociarsi dal relativo account amministratore. Per un account dell'organizzazione, solo l'account amministratore può dissociare un account membro. Per ulteriori informazioni, consulta the section called “Dissociazione degli account dei membri dell'organizzazione”. Per un account invitato manualmente, l'account amministratore o l'account membro possono dissociare l'account. Per ulteriori informazioni, consulta the section called “Dissociazione degli account dei membri” o the section called “Dissociarsi da un account amministratore”. La disassociazione non è richiesta se si utilizza la configurazione centrale perché l'amministratore CSPM di Security Hub può creare una politica che disabilita Security Hub CSPM per account membri specifici.

Quando disabiliti Security Hub CSPM per un account, viene disabilitato solo nella versione corrente. Regione AWS Tuttavia, se utilizzi la configurazione centrale per disabilitare Security Hub CSPM per account specifici, viene disabilitata nella regione di origine e in tutte le regioni collegate.

Per disabilitare Security Hub CSPM, scegli il tuo metodo preferito e segui i passaggi.

Security Hub CSPM console

Segui questi passaggi per disabilitare Security Hub CSPM utilizzando la console.

Per disabilitare Security Hub CSPM

1. Aprire la console CSPM AWS di Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. Nel riquadro di navigazione, in Settings (Impostazioni), scegliere General (Generali).
3. Nella sezione Disabilita Security Hub CSPM, scegli Disabilita Security Hub CSPM.
4. Quando viene richiesta la conferma, scegli Disabilita Security Hub CSPM.

Security Hub API

Per disabilitare Security Hub CSPM a livello di codice, utilizzare il DisableSecurityHubfunzionamento dell'API Security HubAWS. Oppure, se utilizzi il, esegui il comando AWS CLI disable-security-hub. Ad esempio, il comando seguente disabilita Security Hub CSPM nella versione corrente: Regione AWS

```
$ aws securityhub disable-security-hub
```

Sicurezza in AWS Security Hub CSPM

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. Third-partyi revisori testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei programmi di AWS conformità. Per ulteriori informazioni sui programmi di conformità che si applicano a AWS Security Hub CSPM, consulta Servizi coperti dal programma di conformitàAWS.

- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Security Hub CSPM. I seguenti argomenti mostrano come configurare Security Hub CSPM per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le risorse CSPM del Security Hub.

Argomenti

- Protezione dei dati in AWS Security Hub CSPM
- AWS Identity and Access Management per Security Hub CSPM
- Convalida della conformità per AWS Security Hub CSPM
- Resilienza in AWS Security Hub
- Sicurezza dell'infrastruttura in AWS Security Hub CSPM
- AWS Security Hub CSPM e endpoint VPC di interfaccia (AWS PrivateLink)

Protezione dei dati in AWS Security Hub CSPM

Ulteriori informazioni su come il modello di responsabilità condivisa AWS si applica alla protezione dei dati in AWS Security Hub CSPM. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i. Cloud AWS L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati . Per ulteriori informazioni sulla protezione dei dati in Europa, consulta il Centro generale sulla protezione dei dati (GDPR).

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e configurare singoli utenti con Centro identità AWS IAM o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.

- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Security Hub CSPM o altro Servizi AWS utilizzando la console, l'API o AWS gli AWS CLI SDK. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Security Hub CSPM è un'offerta di servizi multi-tenant. Per garantire la protezione dei dati, Security Hub CSPM crittografa i dati inattivi e i dati in transito tra i servizi componenti.

AWS Identity and Access Management per Security Hub CSPM

AWS Identity and Access Management (IAM) è un programma Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse del Security Hub. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso tramite policy
- Come funziona Security Hub con IAM

- Identity-based esempi di politiche per AWS Security Hub CSPM
- Service-linked ruoli per AWS Security Hub CSPM
- AWS politiche gestite per Security Hub
- Risoluzione dei problemi AWS Security Hub CSPM identità e accesso

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi AWS Security Hub CSPM identità e accesso)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta Come funziona Security Hub con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Identity-based esempi di politiche per AWS Security Hub CSPM)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come Centro identità AWS IAM (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare Centro identità AWS IAM. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di Centro identità AWS IAM .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste

politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Identity-based politiche

Identity-based le politiche sono documenti di policy sulle autorizzazioni JSON che alleghi a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Identity-based le politiche possono essere politiche in linea (incorporate direttamente in una singola identità) o politiche gestite (politiche autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Resource-based politiche

Resource-based le politiche sono documenti di policy JSON allegati a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Resource-based le politiche sono politiche in linea che si trovano in quel servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): specifica il numero massimo di autorizzazioni per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di controllo delle risorse (RCP): imposta le autorizzazioni massime disponibili per le risorse degli account. Per ulteriori informazioni, consulta Policy di controllo delle risorse (RCP) nella Guida per l'utente di AWS Organizations .
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Security Hub con IAM

Prima di utilizzare AWS Identity and Access Management (IAM) per gestire l'accesso a AWS Security Hub CSPM, scopri quali funzionalità IAM sono disponibili per l'uso con Security Hub CSPM.

Funzionalità IAM che puoi utilizzare con AWS Security Hub CSPM

Funzionalità IAM	Supporto CSPM Security Hub
Identity-based politiche	Sì
Resource-based politiche	No
Operazioni di policy	Sì
Risorse relative alle policy	No
Chiavi di condizione delle policy	Sì
Liste di controllo accessi di rete (ACL)	No

Funzionalità IAM	Supporto CSPM Security Hub
Attribute-based controllo degli accessi (ABAC): tag nelle politiche	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	No
Service-linked ruoli	Sì

Per una panoramica di alto livello su come Security Hub CSPM e altri Servizi AWS funzionano con la maggior parte delle funzionalità IAM, consulta Servizi AWS That work with IAM nella IAM User Guide.

Identity-based politiche per Security Hub CSPM

Supporta le policy basate sull'identità: sì

Identity-based le policy sono documenti di policy sulle autorizzazioni JSON che è possibile allegare a un'identità, ad esempio un utente IAM, un gruppo di utenti o un ruolo. Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Security Hub CSPM supporta politiche basate sull'identità. Per ulteriori informazioni, consulta Identity-based esempi di politiche per AWS Security Hub CSPM.

Resource-based politiche per Security Hub CSPM

Supporta le policy basate su risorse: no

Resource-based le politiche sono documenti di policy JSON allegati a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei

servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Security Hub CSPM non supporta politiche basate sulle risorse. Non è possibile allegare una policy IAM direttamente a una risorsa CSPM Security Hub.

Azioni politiche per Security Hub CSPM

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Le azioni politiche in Security Hub CSPM utilizzano il seguente prefisso prima dell'azione:

```
securityhub:
```

Ad esempio, per concedere a un utente l'autorizzazione ad abilitare Security Hub CSPM, che è un'azione che corrisponde al `EnableSecurityHub` funzionamento dell'API CSPM di Security Hub, includi l'`securityhub:EnableSecurityHub`azione nella loro politica. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Security Hub CSPM definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

```
"Action": "securityhub:EnableSecurityHub"
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola. Ad esempio:

```
"Action": [
```

```
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

È inoltre possibile specificare più azioni utilizzando caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Get`, includi la seguente azione:

```
"Action": "securityhub:Get*"
```

Tuttavia, è consigliabile definire policy in grado di seguire il principio del privilegio minimo. In altre parole, è necessario creare policy che includano solo le autorizzazioni necessarie per eseguire un'attività specifica.

L'utente deve avere accesso all'`DescribeStandardsControl`operazione per poter accedere a `BatchGetSecurityControlsBatchGetStandardsControlAssociations`, e`ListStandardsControlAssociations`.

L'utente deve avere accesso all'`UpdateStandardsControls`operazione per poter accedere a`BatchUpdateStandardsControlAssociations`, e`UpdateSecurityControl`.

Per un elenco delle azioni CSPM di Security Hub, vedere Azioni definite da AWS Security Hub CSPM nel Service Authorization Reference. Per esempi di politiche che specificano le azioni CSPM di Security Hub, vedere. Identity-based esempi di politiche per AWS Security Hub CSPM

Risorse politiche per Security Hub CSPM

Supporta le risorse di policy: No

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Security Hub CSPM definisce i seguenti tipi di risorse:

- Hub

- Prodotto
- Finding aggregator, noto anche come aggregatore interregionale
- Regola di automazione
- Politica di configurazione

È possibile specificare questi tipi di risorse nelle politiche utilizzando gli ARN.

Per un elenco dei tipi di risorse CSPM di Security Hub e la sintassi ARN per ciascuno di essi, vedere Tipi di risorse definiti da AWS Security Hub CSPM nel Service Authorization Reference. Per sapere quali azioni è possibile specificare per ogni tipo di risorsa, vedere Azioni definite da AWS Security Hub CSPM nel Service Authorization Reference. Per esempi di politiche che specificano le risorse, vedereIdentity-based esempi di politiche per AWS Security Hub CSPM.

Chiavi relative alle condizioni delle policy per Security Hub CSPM

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per un elenco delle chiavi di condizione CSPM di Security Hub, vedere Chiavi di condizione AWS Security Hub CSPM nel Riferimento di autorizzazione del servizio. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, vedere Azioni definite da. AWS Security Hub CSPM Per esempi di politiche che utilizzano chiavi condizionali, consultaIdentity-based esempi di politiche per AWS Security Hub CSPM.

Elenchi di controllo degli accessi (ACL) in Security Hub CSPM

Supporta le ACL: no

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Security Hub CSPM non supporta gli ACL, il che significa che non è possibile collegare un ACL a una risorsa CSPM di Security Hub.

Attribute-based controllo degli accessi (ABAC) con Security Hub CSPM

Supporta ABAC (tag nelle policy): sì

Attribute-based il controllo degli accessi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. È possibile allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

È possibile allegare tag alle risorse CSPM di Security Hub. È inoltre possibile controllare l'accesso alle risorse fornendo informazioni sui tag nell'`Condition`elemento di una policy.

Per informazioni sull'etichettatura delle risorse CSPM di Security Hub, vedere. Taggare le risorse del Security Hub Per un esempio di politica basata sull'identità che controlla l'accesso a una risorsa in base ai tag, vedi. Identity-based esempi di politiche per AWS Security Hub CSPM

Utilizzo di credenziali temporanee con Security Hub CSPM

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. È possibile ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come o. AssumeRoleGetFederationToken

Security Hub CSPM supporta l'uso di credenziali temporanee.

Sessioni di accesso diretto per Security Hub CSPM

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale chiamante an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ad esempio, Security Hub CSPM invia le richieste FAS a valle Servizi AWS quando si integra Security Hub CSPM con AWS Organizations e quando si designa l'account amministratore CSPM di Security Hub delegato per un'organizzazione in Organizations.

Per altre attività, Security Hub CSPM utilizza un ruolo collegato al servizio per eseguire azioni per conto dell'utente. Per i dettagli su questo ruolo, consulta. Service-linked ruoli per AWS Security Hub CSPM

Ruoli di servizio per Security Hub CSPM

Security Hub CSPM non assume né utilizza ruoli di servizio. Per eseguire azioni per conto dell'utente, Security Hub CSPM utilizza un ruolo collegato al servizio. Per i dettagli su questo ruolo, consulta. Service-linked ruoli per AWS Security Hub CSPM

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio può creare problemi operativi con l'uso di Security Hub CSPM. Modifica i ruoli di servizio solo quando Security Hub CSPM fornisce indicazioni in tal senso.

Service-linked ruoli per Security Hub CSPM

Supporta i ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo di eseguire un'azione per conto dell'utente. Service-linked i ruoli vengono

visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Security Hub CSPM utilizza un ruolo collegato al servizio per eseguire azioni per conto dell'utente. Per i dettagli su questo ruolo, consulta. Service-linked ruoli per AWS Security Hub CSPM

Identity-based esempi di politiche per AWS Security Hub CSPM

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse CSPM di Security Hub. Inoltre, non possono eseguire attività utilizzando l'API Console di gestione AWS AWS CLI, o AWS . Un amministratore deve creare le policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore devi quindi collegare queste policy a utenti o gruppi che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente IAM.

Argomenti

- Best practice delle policy
- Utilizzo della console Security Hub CSPM
- Esempio: consentire agli utenti di visualizzare le loro autorizzazioni
- Esempio: consentire agli utenti di creare e gestire una politica di configurazione
- Esempio: consenti agli utenti di visualizzare i risultati
- Esempio: consentire agli utenti di creare e gestire regole di automazione

Best practice delle policy

Identity-based i criteri determinano se qualcuno può creare, accedere o eliminare le risorse del Security Hub nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti

specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Security Hub CSPM

Per accedere alla AWS Security Hub CSPM console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse CSPM di Security Hub presenti nel tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso o l' AWS CLI API. AWS Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che tali utenti e ruoli possano utilizzare la console CSPM di Security Hub, allega anche la seguente politica AWS gestita all'entità. Per ulteriori informazioni, consulta la sezione Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Esempio: consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. 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": "*"
        }
    ]
}
```

Esempio: consentire agli utenti di creare e gestire una politica di configurazione

Questo esempio mostra come è possibile creare una policy IAM che consenta a un utente di creare, visualizzare, aggiornare ed eliminare le politiche di configurazione. Questa policy di esempio consente inoltre all'utente di avviare, interrompere e visualizzare le associazioni di policy. Affinché questa policy IAM funzioni, l'utente deve essere l'amministratore CSPM di Security Hub delegato per un'organizzazione.

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": "*"
        }
    ]
}
```

Esempio: consenti agli utenti di visualizzare i risultati

Questo esempio mostra come è possibile creare una policy IAM che consenta a un utente di visualizzare i risultati del Security Hub CSPM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

Esempio: consentire agli utenti di creare e gestire regole di automazione

Questo esempio mostra come è possibile creare una policy IAM che consenta a un utente di creare, visualizzare, aggiornare ed eliminare le regole di automazione CSPM di Security Hub. Affinché questa policy IAM funzioni, l'utente deve essere un amministratore CSPM di Security Hub. Per limitare le autorizzazioni, ad esempio per consentire a un utente di visualizzare solo le regole di automazione, puoi rimuovere le autorizzazioni di creazione, aggiornamento ed eliminazione.

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 ruoli per AWS Security Hub CSPM

AWS Security Hub CSPM utilizza un ruolo collegato al servizio AWS Identity and Access Management (IAM) denominato. `AWSServiceRoleForSecurityHub` Questo ruolo collegato al servizio è un ruolo IAM collegato direttamente al Security Hub CSPM. È predefinito da Security Hub CSPM e include tutte le autorizzazioni richieste da Security Hub CSPM per chiamare altre persone Servizi AWS e monitorare le risorse per tuo conto. AWS Security Hub CSPM utilizza questo ruolo collegato al servizio in tutti i casi in cui Security Regioni AWS Hub CSPM è disponibile.

Un ruolo collegato al servizio semplifica la configurazione di Security Hub CSPM perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Security Hub CSPM definisce le

autorizzazioni del suo ruolo collegato al servizio e, se non diversamente definito, solo Security Hub CSPM può assumere il ruolo. Le autorizzazioni definite includono la politica di fiducia e la politica delle autorizzazioni e non è possibile collegare tale politica di autorizzazioni a nessun'altra entità IAM.

Per esaminare i dettagli del ruolo collegato al servizio, puoi utilizzare la console Security Hub CSPM. Nel riquadro di navigazione, scegli Generale in Impostazioni. Quindi, nella sezione Autorizzazioni di servizio, scegli Visualizza le autorizzazioni del servizio.

È possibile eliminare il ruolo collegato al servizio Security Hub CSPM solo dopo aver disabilitato Security Hub CSPM in tutte le regioni in cui è abilitato. In questo modo proteggi le tue risorse CSPM di Security Hub perché non puoi rimuovere inavvertitamente le autorizzazioni per accedervi.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta i AWS servizi che funzionano con IAM nella Guida per l'utente di IAM e individua i servizi con Sì nella colonna dei ruoli. Service-linked Scegli un Sì con un link per consultare la documentazione del ruolo collegato al servizio per quel servizio.

Argomenti

- Service-linked autorizzazioni di ruolo per Security Hub CSPM
- Creazione di un ruolo collegato al servizio per Security Hub CSPM
- Modifica di un ruolo collegato al servizio per Security Hub CSPM
- Eliminazione di un ruolo collegato al servizio per Security Hub CSPM

Service-linked autorizzazioni di ruolo per Security Hub CSPM

Security Hub CSPM utilizza il ruolo collegato al servizio denominato. `AWSServiceRoleForSecurityHub` È un ruolo collegato al servizio necessario per accedere alle tue risorse. AWS Security Hub CSPM Questo ruolo collegato al servizio consente a Security Hub CSPM di eseguire attività come ricevere risultati da altri Servizi AWS e configurare l' AWS Config infrastruttura necessaria per eseguire i controlli di sicurezza. Ai fini dell'assunzione del ruolo `AWSServiceRoleForSecurityHub`, il ruolo collegato ai servizi `securityhub.amazonaws.com`considera attendibile il servizio.

Il ruolo collegato ai servizi `AWSServiceRoleForSecurityHub` utilizza la policy gestita `AWSSecurityHubServiceRolePolicy`.

È necessario concedere le autorizzazioni per consentire a un'identità IAM (come un ruolo, un gruppo o un utente) di creare, modificare o eliminare un ruolo collegato al servizio.

`AWSServiceRoleForSecurityHub`Affinché il ruolo collegato al servizio venga creato correttamente, l'identità IAM utilizzata per accedere a Security Hub CSPM deve disporre delle autorizzazioni richieste. Per concedere le autorizzazioni richieste, collega la seguente policy all'identità IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Creazione di un ruolo collegato al servizio per Security Hub CSPM

Il ruolo `AWSServiceRoleForSecurityHub` collegato al servizio viene creato automaticamente quando abiliti Security Hub CSPM per la prima volta o quando abiliti Security Hub CSPM in una regione in cui non lo abilitavi in precedenza. Puoi anche creare il ruolo `AWSServiceRoleForSecurityHub` collegato al servizio manualmente utilizzando la console IAM, la CLI IAM o l'API IAM. Per ulteriori informazioni sulla creazione manuale del ruolo, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM.

> **Important**
>
> Il ruolo collegato al servizio creato per un account amministratore CSPM di Security Hub non si applica agli account membri CSPM di Security Hub associati.

Modifica di un ruolo collegato al servizio per Security Hub CSPM

Security Hub CSPM non consente di modificare il ruolo collegato al `AWSServiceRoleForSecurityHub` servizio. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Security Hub CSPM

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo, non hai un'entità non utilizzata che non viene monitorata o gestita attivamente.

Quando disabiliti Security Hub CSPM, Security Hub CSPM non elimina automaticamente il ruolo collegato al `AWSServiceRoleForSecurityHub` servizio per te. Se abiliti nuovamente Security Hub CSPM, il servizio può ricominciare a utilizzare il ruolo esistente collegato al servizio. Se non è più necessario utilizzare Security Hub CSPM, è possibile eliminare manualmente il ruolo collegato al servizio.

> **Important**
>
> Prima di eliminare il ruolo `AWSServiceRoleForSecurityHub` collegato al servizio, devi prima disabilitare Security Hub CSPM in tutte le regioni in cui è abilitato. Per ulteriori informazioni, consulta Disattivazione del Security Hub CSPM. Se Security Hub CSPM non è disabilitato quando si tenta di eliminare il ruolo collegato al servizio, l'eliminazione non riesce.

Per eliminare il ruolo `AWSServiceRoleForSecurityHub` collegato al servizio, puoi utilizzare la console IAM, la CLI IAM o l'API IAM. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

AWS politiche gestite per Security Hub

Una politica AWS gestita è una politica autonoma creata e amministrata da. AWS AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

AWS politica gestita: AWSSecurityHubFullAccess

È possibile allegare la policy `AWSSecurityHubFullAccess` alle identità IAM.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo principale a tutte le azioni CSPM di Security Hub. Questa politica deve essere associata a un principale prima che quest'ultimo abiliti manualmente Security Hub CSPM per il proprio account. Ad esempio, i responsabili con queste autorizzazioni possono sia visualizzare che aggiornare lo stato dei risultati. Possono anche configurare approfondimenti personalizzati, abilitare integrazioni e abilitare e disabilitare standard e controlli. I responsabili di un account amministratore possono anche gestire gli account dei membri.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `securityhub`— Consente ai responsabili l'accesso completo a tutte le azioni CSPM di Security Hub.
- `guardduty`— Consente ai responsabili di eseguire la gestione completa del ciclo di vita di un rilevatore, la gestione degli amministratori dell'organizzazione, la gestione degli account

dei membri e la configurazione a livello di organizzazione in Amazon. GuardDuty Ciò include le azioni API: GetDetector,,,,,,, ListDetector. CreateDetector UpdateDetector DeleteDetector EnableOrganizationAdminAccount ListOrganizationAdminAccounts CreateMembers UpdateOrganizationConfiguration DescribeOrganizationConfiguration

- `iam`— Consente ai responsabili di creare un ruolo collegato ai servizi per Security Hub CSPM e Security Hub e di ottenere ruoli, policy e versioni di policy.
- `inspector`— Consente ai responsabili di ottenere informazioni sullo stato dell'account, abilitare o disabilitare, delegare la gestione amministrativa ed eseguire la gestione della configurazione dell'organizzazione in Amazon Inspector. Ciò include le azioni API: BatchGetAccountStatus, Abilita,,,, EnableDelegatedAdminAccount DisableDelegatedAdminAccount, ListDelegatedAdminAccounts. UpdateOrganizationConfiguration DescribeOrganizationConfiguration
- `pricing`— Consente ai committenti di ottenere un listino prezzi Servizi AWS e prodotti.
- `account`— Consente ai responsabili di ottenere informazioni sulle regioni degli account per supportare la gestione delle regioni in Security Hub.

Per esaminare le autorizzazioni relative a questa politica, consulta AWSSecurityHubFullAccessla AWS Managed Policy Reference Guide.

AWS politica gestita: AWSSecurityHubReadOnlyAccess

È possibile allegare la policy `AWSSecurityHubReadOnlyAccess` alle identità IAM.

Questa politica concede autorizzazioni di sola lettura che consentono agli utenti di visualizzare le informazioni in Security Hub CSPM. I responsabili a cui è allegata questa politica non possono effettuare aggiornamenti in Security Hub CSPM. Ad esempio, i responsabili con queste autorizzazioni possono visualizzare l'elenco dei risultati associati al proprio account, ma non possono modificare lo stato di un risultato. Possono visualizzare i risultati degli approfondimenti, ma non possono creare o configurare approfondimenti personalizzati. Non possono configurare controlli o integrazioni di prodotti.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `securityhub`— Consente agli utenti di eseguire azioni che restituiscono un elenco di elementi o dettagli su un elemento. Ciò include le operazioni API che iniziano con `GetList`, o`Describe`.

Per esaminare le autorizzazioni relative a questa policy, consulta AWSSecurityHubReadOnlyAccessla AWS Managed Policy Reference Guide.

AWS politica gestita: AWSSecurityHubOrganizationsAccess

È possibile allegare la policy `AWSSecurityHubOrganizationsAccess` alle identità IAM.

Questa politica concede le autorizzazioni amministrative per abilitare e gestire Security Hub, Security Hub CSPM, Amazon e GuardDuty Amazon Inspector per un'organizzazione in. AWS Organizations Le autorizzazioni per questa politica consentono all'account di gestione dell'organizzazione di designare l'account amministratore delegato per Security Hub, Security Hub CSPM, Amazon e GuardDuty Amazon Inspector. Consentono inoltre all'account amministratore delegato di abilitare gli account dell'organizzazione come account membro.

Questa politica fornisce solo le autorizzazioni per. AWS Organizations L'account di gestione dell'organizzazione e l'account amministratore delegato richiedono inoltre le autorizzazioni per le azioni associate. Queste autorizzazioni possono essere concesse utilizzando la politica gestita`AWSSecurityHubFullAccess`.

La creazione o l'aggiornamento di una politica di amministratore delegato in un account di gestione richiede autorizzazioni aggiuntive non fornite in questa politica. Per eseguire queste azioni si consiglia di aggiungere autorizzazioni `organizations:PutResourcePolicy` o allegare la politica. AWSOrganizationsFullAccess

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `organizations:ListAccounts`— Consente ai responsabili di recuperare l'elenco degli account che fanno parte di un'organizzazione.
- `organizations:DescribeOrganization`— Consente ai dirigenti di recuperare informazioni sull'organizzazione.
- `organizations:ListRoots`— Consente ai dirigenti di elencare la radice di un'organizzazione.
- `organizations:ListDelegatedAdministrators`— Consente ai dirigenti di elencare l'amministratore delegato di un'organizzazione.
- `organizations:ListAWSServiceAccessForOrganization`— Consente ai dirigenti di elencare le informazioni utilizzate da un' Servizi AWS organizzazione.
- `organizations:ListOrganizationalUnitsForParent`— Consente ai responsabili di elencare le unità organizzative (OU) secondarie di un'unità organizzativa principale.

- `organizations:ListAccountsForParent`— Consente ai responsabili di elencare gli account secondari di un'unità organizzativa principale.
- `organizations:ListParents`— Elenca le unità organizzative o principali (OU) che fungono da elemento principale dell'unità organizzativa o dell'account figlio specificato.
- `organizations:DescribeAccount`: consente ai principali di recuperare informazioni su un account nell'organizzazione.
- `organizations:DescribeOrganizationalUnit`— Consente ai responsabili di recuperare informazioni su un'unità organizzativa all'interno dell'organizzazione.
- `organizations:ListPolicies`— Recupera l'elenco di tutte le politiche di un'organizzazione di un tipo specificato.
- `organizations:ListPoliciesForTarget`— Elenca le politiche direttamente collegate alla radice, all'unità organizzativa (OU) o all'account di destinazione specificati.
- `organizations:ListTargetsForPolicy`— Elenca tutte le radici, le unità organizzative (OU) e gli account a cui è associata la politica specificata.
- `organizations:EnableAWSServiceAccess`— Consente ai presidi di abilitare l'integrazione con Organizations.
- `organizations:RegisterDelegatedAdministrator`— Consente ai responsabili di designare l'account amministratore delegato.
- `organizations:DeregisterDelegatedAdministrator`— Consente ai responsabili di rimuovere l'account amministratore delegato.
- `organizations:DescribePolicy`— Recupera informazioni su una politica.
- `organizations:DescribeEffectivePolicy`— Restituisce il contenuto della politica effettiva per il tipo di politica e l'account specificati.
- `organizations:CreatePolicy`— Crea una politica di un tipo specifico che è possibile allegare a una radice, a un'unità organizzativa (OU) o a un AWS account individuale.
- `organizations:UpdatePolicy`— Aggiorna una politica esistente con un nuovo nome, descrizione o contenuto.
- `organizations:DeletePolicy`— Elimina la politica specificata dall'organizzazione.
- `organizations:AttachPolicy`— Associa una policy a una root, a un'unità organizzativa (OU) o a un account individuale.
- `organizations:DetachPolicy`— Scollega una politica da una radice, un'unità organizzativa (OU) o un account di destinazione.
- `organizations:EnablePolicyType`— Abilita un tipo di policy in una radice.

- `organizations:DisablePolicyType`— Disattiva un tipo di politica organizzativa in una radice.
- `organizations:TagResource`— Aggiunge uno o più tag a una risorsa specificata.
- `organizations:UntagResource`— Rimuove tutti i tag con le chiavi specificate da una risorsa specificata.
- `organizations:ListTagsForResource`— Elenca i tag allegati a una risorsa specificata.
- `organizations:DescribeResourcePolicy`— Recupera informazioni su una politica delle risorse.

Per esaminare le autorizzazioni relative a questa politica, vedere AWSSecurityHubOrganizationsAccessla AWS Managed Policy Reference Guide.

AWS politica gestita: AWSSecurityHubServiceRolePolicy

Non è possibile collegare `AWSSecurityHubServiceRolePolicy`alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente a Security Hub CSPM di eseguire azioni per conto dell'utente. Per ulteriori informazioni, consulta the section called "Service-linked ruoli".

Questa politica concede autorizzazioni amministrative che consentono al ruolo collegato al servizio di eseguire attività come eseguire controlli di sicurezza per i controlli CSPM di Security Hub.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `cloudtrail`— Recupera informazioni sui sentieri. CloudTrail
- `cloudwatch`— Recupera gli CloudWatch allarmi correnti e le metriche sullo stato del connettore.
- `logs`— Recupera i filtri metrici per i log. CloudWatch
- `sns`— Recupera l'elenco delle sottoscrizioni a un argomento SNS.
- `config`— Recupera informazioni sui registratori di configurazione, sulle risorse e sulle regole. AWS Config Gestisci i registratori di configurazione collegati al servizio Security Hub CSPM e i registratori di configurazione collegati ai servizi di terze parti. Crea ed elimina AWS Config regole ed esegui valutazioni in base alle regole. Elenca i registratori di configurazione e ottieni informazioni sui connettori per supportare integrazioni cloud di terze parti.
- `iam`— Recupera e genera report sulle credenziali per gli account e crea il ruolo collegato al servizio per. AWS Config
- `organizations`— Recupera informazioni sull'account e sull'unità organizzativa (OU) di un'organizzazione.

- `securityhub`— Recupera informazioni su come sono configurati il servizio CSPM, gli standard e i controlli di Security Hub.
- `tag`— Recupera informazioni sui tag delle risorse.

Per esaminare le autorizzazioni relative a questa politica, consulta AWSSecurityHubServiceRolePolicyla AWS Managed Policy Reference Guide.

Aggiornamenti del Security Hub a AWS policy gestite

La tabella seguente fornisce dettagli sugli aggiornamenti alle politiche AWS gestite per AWS Security Hub e Security Hub CSPM da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sugli aggiornamenti delle politiche, iscriviti al feed RSS nella pagina della cronologia dei documenti di Security Hub.

Modifica	Descrizione	Data
AWSSecurityHubServiceRolePolicy— Politica aggiornata	Security Hub CSPM ha aggiornato la politica per supportare l'integrazione di terze parti. L'aggiornamento aggiunge le seguenti autorizzazioni: gestire i registratori di configurazione di terze parti, elencare i registratori di configurazione, ottenere informazioni sui connettori e recuperare le metriche sullo stato del connettore.	30 giugno 2026
AWSSecurityHubServiceRolePolicy— Politica aggiornata	Security Hub CSPM ha aggiornato la policy per aggiungere le autorizzazioni per gestire i registratori di configurazione collegati al servizio Security Hub CSPM	29 aprile 2026

Modifica	Descrizione	Data
	e creare il ruolo collegato al servizio. AWS Config	
AWSSecurityHubOrganizationsAccess— Politica aggiornata	Security Hub ha aggiornato la politica per aggiungere autorizzazioni per descrivere le politiche delle risorse per supportare le funzionalità di Security Hub. Security Hub è in versione di anteprima ed è soggetto a modifiche.	12 novembre 2025
AWSSecurityHubFullAccess— Politica aggiornata	Security Hub ha aggiornato la policy per aggiungere funzionalità di gestione GuardDuty, Amazon Inspector e gestione degli account per supportare le funzionalità di Security Hub. Security Hub è in versione di anteprima ed è soggetto a modifiche.	17 novembre 2025
AWSSecurityHubOrganizationsAccess: aggiornamento di una policy esistente	Security Hub ha aggiunto nuove autorizzazioni alla policy. Le autorizzazioni consentono alla direzione dell'organizzazione di abilitare e gestire Security Hub e Security Hub CSPM per un'organizzazione.	17 giugno 2025
AWSSecurityHubFullAccess: aggiornamento di una policy esistente	Security Hub CSPM ha aggiunto nuove autorizzazioni che consentono ai responsabili di creare un ruolo collegato al servizio per Security Hub.	17 giugno 2025

Modifica	Descrizione	Data
AWSSecurityHubFullAccess— Aggiornamento a una politica esistente	Security Hub CSPM ha aggiornato la politica per ottenere dettagli sui prezzi Servizi AWS e sui prodotti.	24 aprile 2024
AWSSecurityHubReadOnlyAccess— Aggiornamento a una politica esistente	Security Hub CSPM ha aggiornato questa politica gestita aggiungendo un `Sid` campo.	22 febbraio 2024
AWSSecurityHubFullAccess— Aggiornamento a una politica esistente	Security Hub CSPM ha aggiornato la policy in modo da determinare se Amazon GuardDuty e Amazon Inspector sono abilitati in un account. Questo aiuta i clienti a riunire più informazioni relative alla sicurezza. Servizi AWS	16 novembre 2023
AWSSecurityHubOrganizationsAccess— Aggiornamento a una politica esistente	Security Hub CSPM ha aggiornato la politica per concedere autorizzazioni aggiuntive per consentire l'accesso in sola lettura alle funzionalità di amministratore delegato. AWS Organizations Ciò include dettagli come la radice, le unità organizzative (OU), gli account, la struttura organizzativa e l'accesso al servizio.	16 novembre 2023

Modifica	Descrizione	Data
AWSSecurityHubServiceRolePolicy: aggiornamento di una policy esistente	Security Hub CSPM ha aggiunto le `BatchGetSecurityControls` autorizzazioni e `UpdateSecurityControl` le autorizzazioni per leggere e aggiornare le proprietà di controllo di sicurezza personalizzabili. `DisassociateFromAdministratorAccount`	26 novembre 2023
AWSSecurityHubServiceRolePolicy: aggiornamento di una policy esistente	Security Hub CSPM ha aggiunto l'`tag:GetResources` autorizzazione a leggere i tag delle risorse relativi ai risultati.	7 novembre 2023
AWSSecurityHubServiceRolePolicy: aggiornamento di una policy esistente	Security Hub CSPM ha aggiunto l'`BatchGetStandardsControlAssociations` autorizzazione per ottenere informazioni sullo stato di abilitazione di un controllo in uno standard.	27 settembre 2023
AWSSecurityHubServiceRolePolicy: aggiornamento di una policy esistente	Security Hub CSPM ha aggiunto nuove autorizzazioni per ottenere AWS Organizations dati e leggere e aggiornare le configurazioni CSPM di Security Hub, inclusi standard e controlli.	20 settembre 2023

Modifica	Descrizione	Data
AWSSecurityHubServiceRolePolicy: aggiornamento di una policy esistente	Security Hub CSPM ha spostato l'`config:DescribeConfigRuleEvaluationStatus` autorizzazione esistente in una dichiarazione diversa all'interno della politica. L'`config:DescribeConfigRuleEvaluationStatus` autorizzazione viene ora applicata a tutte le risorse.	17 marzo 2023
AWSSecurityHubServiceRolePolicy: aggiornamento di una policy esistente	Security Hub CSPM ha spostato l'`config:PutEvaluations` autorizzazione esistente in una dichiarazione diversa all'interno della politica. L'`config:PutEvaluations` autorizzazione viene ora applicata a tutte le risorse.	14 luglio 2021
AWSSecurityHubServiceRolePolicy: aggiornamento di una policy esistente	Security Hub CSPM ha aggiunto una nuova autorizzazione per consentire al ruolo collegato al servizio di fornire risultati di valutazione. AWS Config	29 giugno 2021
AWSSecurityHubServiceRolePolicy— Aggiunto all'elenco delle politiche gestite	Sono state aggiunte informazioni sulla policy gestita AWSSecurityHubServiceRolePolicy, utilizzata dal ruolo collegato al servizio Security Hub CSPM.	11 giugno 2021

Modifica	Descrizione	Data
AWSSecurityHubOrganizationsAccess— Nuova politica	Security Hub CSPM ha aggiunto una nuova politica che concede le autorizzazioni necessarie per l'integrazione del Security Hub CSPM con Organizations.	15 marzo 2021
Security Hub CSPM ha iniziato a tracciare le modifiche	Security Hub CSPM ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	15 marzo 2021

Risoluzione dei problemi AWS Security Hub CSPM identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS Security Hub CSPM un IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Security Hub CSPM
- Non sono autorizzato a eseguire iam: PassRole
- Desidero l'accesso programmatico a Security Hub CSPM
- Sono un amministratore e desidero consentire ad altri di accedere a Security Hub CSPM
- Voglio consentire l'accesso a persone esterne al mio Account AWS per accedere alle mie risorse CSPM Security Hub

Non sono autorizzato a eseguire un'azione in Security Hub CSPM

Se ti Console di gestione AWS dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` tenta di utilizzare la console per visualizzare i dettagli su un *`widget`* ma non dispone `securityhub:`*`GetWidget`* delle autorizzazioni.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

In questo caso, Mateo chiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *my-example-widget* mediante l'operazione `securityhub:GetWidget`.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a Security Hub.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Security Hub. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Desidero l'accesso programmatico a Security Hub CSPM

Gli utenti hanno bisogno di un accesso programmatico se vogliono interagire con AWS l'esterno di. Console di gestione AWS Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Consigliato) Utilizza le credenziali della console come credenziali temporanee per firmare le richieste programmatiche agli AWS SDK o alle AWS CLI API. AWS	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta Login for AWS local development nella Guida per l'utente.AWS Command Line Interface • Per gli AWS SDK, consulta Login per lo sviluppo AWS locale nella Guida di riferimento agli AWS SDK e agli strumenti.
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporanee per firmare le richieste programmatiche agli AWS SDK o alle AWS CLI API. AWS	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta Configurazione dell'uso Centro identità AWS IAM nella Guida AWS CLI per l'utente.AWS Command Line Interface • Per AWS SDK, strumenti e AWS API, consulta l'autenticazione IAM Identity Center nella Guida di riferimento agli AWS SDK e agli strumenti.
IAM	Utilizza credenziali temporanee per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS	Segui le istruzioni in Uso delle credenziali temporanee con AWS risorse nella Guida per l'utente IAM.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface • Per gli AWS SDK e gli strumenti, consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimento agli SDK e agli AWS strumenti. • Per le AWS API, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.

Sono un amministratore e desidero consentire ad altri di accedere a Security Hub CSPM

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- Utenti e gruppi in: Centro identità AWS IAM

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di Centro identità AWS IAM .
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Create a role for a third-party identity provider (federation) della Guida per l'utente IAM.
- Utenti IAM:

- Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina Create a role for an IAM user della Guida per l'utente IAM.
- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

Voglio consentire l'accesso a persone esterne al mio Account AWS per accedere alle mie risorse CSPM Security Hub

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizzare tali policy per concedere alle persone l'accesso alle proprie risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Security Hub supporta queste funzionalità, vedereCome funziona Security Hub con IAM.
- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente di IAM.

Convalida della conformità per AWS Security Hub CSPM

La nostra nuova esperienza di AWS registrazione non è progettata per carichi di lavoro regolamentati. Se utilizzi la nostra nuova esperienza di AWS registrazione, ma desideri utilizzarla AWS per carichi di lavoro regolamentati, puoi iscriverti a AWS (avanzata) o attivare funzionalità avanzate per il tuo ambiente. AWS

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Ambito per programma di conformitàServizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta la Documentazione AWS sulla sicurezza.

Resilienza in AWS Security Hub

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone Regioni AWS di disponibilità, vedere AWS Global Infrastructure.

Sicurezza dell'infrastruttura in AWS Security Hub CSPM

In quanto servizio gestito, AWS Security Hub CSPM è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Si utilizzano chiamate API AWS pubblicate per accedere a Security Hub CSPM attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di crittografia con Perfect Forward Secrecy (PFS) come DHE (Ephemeral) o ECDHE (Elliptic Curve Diffie-Hellman Ephemeral). Diffie-Hellman La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

AWS Security Hub CSPM e endpoint VPC di interfaccia (AWS PrivateLink)

Puoi stabilire una connessione privata tra il tuo VPC e creare un AWS Security Hub CSPM endpoint VPC di interfaccia. Gli endpoint di interfaccia sono alimentati da AWS PrivateLink, una tecnologia che consente di accedere in modo privato alle API CSPM di Security Hub senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione Direct Connect. AWS Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare con le API CSPM di Security Hub. Il traffico tra il tuo VPC e il CSPM di Security Hub non esce dalla rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più interfacce di rete elastiche nelle sottoreti. Per ulteriori informazioni, consulta Accedere a un endpoint VPC Servizio AWS con interfaccia nella Amazon Virtual Private Cloud Guide.

Considerazioni sugli endpoint VPC CSPM di Security Hub

Prima di configurare un endpoint VPC di interfaccia per Security Hub CSPM, assicurati di rivedere i prerequisiti e altre informazioni nella Amazon Virtual Private Cloud Guide.

Security Hub CSPM supporta l'esecuzione di chiamate a tutte le sue azioni API dal tuo VPC.

Creazione di un endpoint VPC di interfaccia per Security Hub CSPM

Puoi creare un endpoint VPC per il servizio CSPM di Security Hub utilizzando la console Amazon VPC o il (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta Creare un endpoint VPC nella Amazon Virtual Private Cloud Guide.

Crea un endpoint VPC per Security Hub CSPM utilizzando il seguente nome di servizio:

`com.amazonaws.`*`region`*`.securityhub`

*`region`*Dov'è il codice regionale applicabile. Regione AWS

Se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API a Security Hub CSPM utilizzando il nome DNS predefinito per la regione, `securityhub.us-east-1.amazonaws.com` ad esempio per la regione Stati Uniti orientali (Virginia settentrionale).

Creazione di una policy per gli endpoint VPC per Security Hub (CSPM)

Puoi allegare una policy per gli endpoint al tuo endpoint VPC che controlla l'accesso a Security Hub CSPM. La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire azioni.

Per ulteriori informazioni, consulta Controllare l'accesso agli endpoint VPC utilizzando le policy degli endpoint nella Amazon Virtual Private Cloud Guide.

Esempio: policy degli endpoint VPC per le azioni CSPM di Security Hub

Di seguito è riportato un esempio di policy degli endpoint per Security Hub CSPM. Se collegata a un endpoint, questa politica consente l'accesso alle azioni CSPM di Security Hub elencate per tutti i principali su tutte le risorse.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Sottoreti condivise

Non puoi creare, descrivere, modificare o eliminare gli endpoint VPC nelle sottoreti condivise con te. Tuttavia, puoi utilizzare gli endpoint VPC in sottoreti condivise con te. Per informazioni sulla condivisione VPC, consulta Condividi le tue sottoreti VPC con altri account nella Amazon Virtual Private Cloud Guide.

Registrazione delle chiamate API Security Hub con CloudTrail

AWSSecurity Hub CSPM è integrato conAWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Security Hub CSPM. CloudTrail

acquisisce le chiamate API per Security Hub CSPM come eventi. Le chiamate acquisite includono chiamate dalla console CSPM di Security Hub e chiamate in codice alle operazioni dell'API CSPM di Security Hub. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Security Hub CSPM. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti sulla CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni CloudTrail raccolte, è possibile determinare la richiesta effettuata a Security Hub CSPM, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per saperne di più CloudTrail, incluso come configurarlo e abilitarlo, consulta la Guida per l'AWS CloudTrailutente.

Informazioni CSPM di Security Hub in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività di evento supportata in Security Hub CSPM, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account . Per ulteriori informazioni, vedere Visualizzazione degli eventi con CloudTrail la cronologia degli eventi.

Per una registrazione continua degli eventi nel tuo account, inclusi gli eventi per Security Hub CSPM, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un trail nella console, il trail si applica a tutte le regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Security Hub CSPM supporta la registrazione di tutte le azioni dell'API CSPM di Security Hub come eventi nei registri. CloudTrail Per visualizzare un elenco delle operazioni CSPM di Security Hub, consulta il riferimento all'API CSPM di Security Hub.

Quando viene registrata l'attività per le seguenti azioni CloudTrail, il valore di è impostato su. `responseElements` `null` Ciò garantisce che le informazioni sensibili non siano incluse nei CloudTrail registri.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM)
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Esempio: voci del file di registro CSPM di Security Hub

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreateInsight`azione. In questo esempio, viene creata un'informazione dettagliata denominata `Test Insight`. L'attributo `ResourceId` viene specificato come l'aggregatore Group by (Raggruppa per) e non viene specificato alcun filtro opzionale per questa informazione dettagliata. Per ulteriori informazioni sulle informazioni dettagliate, consulta Visualizzazione degli approfondimenti in Security Hub CSPM.

```
{
```

```
    "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"
}
```

Taggare le risorse del Security Hub

Un tag è un'etichetta opzionale che è possibile definire e assegnare alle AWS risorse, inclusi alcuni tipi di risorse CSPM di AWS Security Hub. I tag consentono di identificare, categorizzare e gestire le risorse in diversi modi, ad esempio in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Ad esempio, è possibile utilizzare i tag per distinguere le risorse, identificare le risorse che supportano determinati requisiti o flussi di lavoro di conformità o allocare i costi.

È possibile aggiungere tag ai seguenti tipi di risorse CSPM di Security Hub:

- Regole di automazione
- Policy di configurazione
- Risorsa Hub

Nozioni fondamentali sull'etichettatura

Una risorsa può avere fino a 50 tag. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale, entrambi definibili dall'utente. Una chiave di tag è un'etichetta generale che funge da categoria per un valore di tag più specifico. Un valore di tag funge da descrittore di una chiave di tag.

Ad esempio, se si creano regole di automazione diverse per ambienti diversi (un set di regole di automazione per gli account di test e un altro per gli account di produzione), è possibile assegnare una chiave di `Environment` tag a tali regole. Il valore del tag associato potrebbe `Test` riferirsi alle regole associate agli account di test e alle regole associate `Prod` agli account di produzione e alle unità organizzative.

Durante la definizione e l'assegnazione di tag alle risorse CSPM AWS di Security Hub, tenete presente quanto segue:

- Ogni risorsa può avere un massimo di 50 tag.
- Per ogni risorsa, ogni chiave di tag deve essere unica e può avere un solo valore di tag.
- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole. Come best practice, ti consigliamo di definire una strategia per utilizzare i tag in maiuscolo e di implementarla in modo coerente tra le tue risorse.

- Una chiave tag può contenere un massimo di 128 UTF-8 caratteri. Il valore di un tag può contenere un massimo di 256 UTF-8 caratteri. I caratteri possono essere lettere, numeri, spazi o i seguenti simboli: _.:/= + - @
- Il `aws:` prefisso è riservato all'uso diAWS. Non puoi usarlo in nessuna chiave o valore di tag che definisci. Inoltre, non è possibile modificare o rimuovere le chiavi o i valori dei tag che utilizzano questo prefisso. I tag che utilizzano questo prefisso non vengono conteggiati per la quota di 50 tag per ogni risorsa.
- Tutti i tag che assegni sono disponibili solo per te Account AWS e solo nel gruppo Regione AWS in cui li assegni.
- Se si assegnano tag a una risorsa utilizzando Security Hub CSPM, i tag vengono applicati solo alla risorsa archiviata direttamente in Security Hub CSPM nel paese applicabile. Regione AWS Non vengono applicati alle risorse di supporto associate che Security Hub CSPM crea, utilizza o gestisce per te in altri. Servizi AWS Ad esempio, se assegni tag a una regola di automazione che aggiorna i risultati relativi ad Amazon Simple Storage Service (Amazon S3), i tag vengono applicati solo alla regola di automazione in Security Hub CSPM per la regione specificata. Non vengono applicati ai tuoi bucket S3. Per assegnare tag anche a una risorsa associata, puoi utilizzare AWS Resource Groups o Servizio AWS quello che memorizza la risorsa, ad esempio Amazon S3 per un bucket S3. L'assegnazione di tag alle risorse associate può aiutarti a identificare le risorse di supporto per le tue risorse CSPM di Security Hub.
- Se si elimina una risorsa, vengono eliminati anche tutti i tag assegnati alla risorsa.

> **Important**
>
> Non archiviate dati riservati o di altro tipo nei tag. I tag sono accessibili da moltiServizi AWS, tra cuiGestione costi e fatturazione AWS. Non sono destinati a essere utilizzati per dati sensibili.

Per aggiungere e gestire i tag per le risorse CSPM di Security Hub, è possibile utilizzare la console CSPM di Security Hub, l'API CSPM di Security Hub o l'API Tagging. AWS Resource Groups Con Security Hub CSPM, puoi aggiungere tag a una risorsa quando la crei. È inoltre possibile aggiungere e gestire tag per singole risorse esistenti. Con Resource Groups, puoi aggiungere e gestire tag in blocco per più risorse esistenti su più risorse esistentiServizi AWS, incluso Security Hub CSPM.

Per ulteriori suggerimenti e best practice sull'etichettatura, consulta Tagging your resources nella Tagging AWS Resources User Guide. AWS

Utilizzo di tag nelle policy IAM

Dopo aver iniziato a taggare le risorse, puoi definire autorizzazioni a livello di risorsa basate su tag nelle policy (IAM). AWS Identity and Access Management Utilizzando i tag in questo modo, puoi implementare un controllo granulare su quali utenti e ruoli all'interno dell'azienda Account AWS sono autorizzati a creare e contrassegnare risorse e quali utenti e ruoli sono autorizzati ad aggiungere, modificare e rimuovere tag più in generale. Per controllare l'accesso in base ai tag, puoi utilizzare le chiavi di condizione relative ai tag nell'elemento Condition delle politiche IAM.

Ad esempio, puoi creare una policy IAM che consenta a un utente di avere accesso completo a tutte le risorse CSPM di AWS Security Hub, se il `Owner` tag per la risorsa specifica il suo nome utente:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
 "${aws:username}"}
            }
        }
    ]
}
```

Se vengono definite autorizzazioni a livello di risorsa basate su tag, le autorizzazioni diventano subito effettive. Ciò significa che le risorse sono più sicure non appena vengono create e che è possibile avviare rapidamente l'applicazione di tag alle nuove risorse. È inoltre possibile utilizzare le autorizzazioni a livello di risorsa per controllare quali chiavi e valori di tag possono essere associati a risorse nuove ed esistenti. Per ulteriori informazioni, consulta Controlling access to AWS resources using tags nella IAM User Guide.

Aggiungere tag alle risorse CSPM di Security Hub

Un tag è un'etichetta che è possibile definire e assegnare alle AWS risorse, inclusi alcuni tipi di risorse CSPM di AWS Security Hub. Utilizzando i tag, è possibile identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Ad esempio, puoi utilizzare i tag per: applicare politiche, allocare i costi, distinguere tra versioni delle risorse o identificare risorse che supportano determinati requisiti o flussi di lavoro di conformità.

È possibile aggiungere tag ai seguenti tipi di risorse CSPM di Security Hub:

- Regole di automazione
- Policy di configurazione
- Risorsa Hub

Una risorsa può avere fino a 50 tag. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. Una chiave tag è un'etichetta generale che funge da categoria per un valore di tag più specifico. Un valore di tag funge da descrittore di una chiave di tag. Per ulteriori informazioni sulle opzioni e sui requisiti di etichettatura, consultaNozioni fondamentali sull'etichettatura.

Per aggiungere tag a una risorsa CSPM di Security Hub, è possibile utilizzare la console CSPM di Security Hub o l'API CSPM di Security Hub. Tuttavia, la console non supporta l'aggiunta di tag alla risorsa. Hub

Dopo aver aggiunto i tag, puoi modificare il tag e cambiare la chiave o il valore del tag.

Per aggiungere o modificare tag per più risorse CSPM di Security Hub contemporaneamente, utilizza le operazioni di tagging dell'API Tagging. AWS Resource Groups

> **Important**
>
> L'aggiunta di tag a una risorsa può influire sull'accesso alla risorsa. Prima di aggiungere un tag a una risorsa, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare i tag per controllare l'accesso alle risorse.

Console

Per aggiungere tag a una risorsa CSPM di Security Hub (console)

Quando si crea una regola di automazione o una politica di configurazione, la console Security Hub CSPM offre opzioni per aggiungere tag. È possibile fornire la chiave e il valore del tag nella sezione Tag.

Security Hub CSPM API

Per aggiungere tag a una risorsa CSPM (API) di Security Hub

Per creare una risorsa e aggiungervi uno o più tag a livello di codice, utilizzate l'operazione appropriata per il tipo di risorsa che desiderate creare:

- Per creare una politica di configurazione e aggiungervi uno o più tag, richiamate l'CreateConfigurationPolicyAPI o, se utilizzate laAWS CLI, eseguite il comando create-configuration-policy.
- Per creare una regola di automazione e aggiungervi uno o più tag, richiama l'CreateAutomationRuleAPI o, se utilizzi il, esegui il comando create-automation-rule. AWS CLI
- Per abilitare Security Hub CSPM e aggiungere uno o più tag alla tua Hub risorsa, richiama l'EnableSecurityHubAPI o, se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando enable-security-hub.

Nella richiesta, utilizzate il `tags` parametro per specificare la chiave del tag e il valore del tag opzionale per ogni tag da aggiungere alla risorsa. Il `tags` parametro specifica una matrice di oggetti. Ogni oggetto specifica una chiave di tag e il relativo valore di tag associato.

Per aggiungere uno o più tag a una risorsa esistente, utilizza l'TagResourceoperazione dell'API CSPM Security Hub o, se utilizzi ilAWS CLI, esegui il comando tag-resource. Nella richiesta, specifica l'Amazon Resource Name (ARN) della risorsa a cui desideri aggiungere un tag. Utilizza il `tags` parametro per specificare la chiave del tag (`key`) e il valore del tag opzionale (`value`) per ogni tag da aggiungere. Il `tags` parametro specifica una matrice di oggetti, un oggetto per ogni chiave di tag e il valore del tag associato.

Ad esempio, il AWS CLI comando seguente aggiunge una chiave di `Environment` tag con un valore di `Prod` tag alla politica di configurazione specificata. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

Esempio di comando CLI:

```
$ aws securityhub tag-resource \
```

```
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod"}'
```

Dove:

- `resource-arn`specifica l'ARN della politica di configurazione a cui aggiungere un tag.
- *`Environment`*è la chiave del tag da aggiungere alla regola.
- *`Prod`*è il valore del tag per la chiave del tag specificata (*`Environment`*).

Nell'esempio seguente, il comando aggiunge diversi tag alla politica di configurazione.

```
$ 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"}'
```

Per ogni oggetto di una `tags` matrice, sono obbligatori `key` sia gli `value` argomenti che. Tuttavia, il valore dell'`value`argomento può essere una stringa vuota. Se non desiderate associare un valore di tag a una chiave di tag, non specificate un valore per l'`value`argomento. Ad esempio, il comando seguente aggiunge una chiave di `Owner` tag senza alcun valore di tag associato:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Se un'operazione di tagging ha esito positivo, Security Hub CSPM restituisce una risposta HTTP 200 vuota. Altrimenti, Security Hub CSPM restituisce una risposta HTTP 4 xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Modifica dei tag per le risorse CSPM di Security Hub

Man mano che l'ambiente o i requisiti cambiano nel tempo, puoi valutare i tag esistenti per le risorse CSPM di AWS Security Hub e modificarli se necessario. Un tag è un'etichetta che definisci e assegni a una o più AWS risorse, inclusi determinati tipi di risorse Macie. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. Una chiave tag è un'etichetta generale che funge

da categoria per un valore di tag più specifico. Un valore di tag funge da descrittore di una chiave di tag.

I tag consentono di identificare, categorizzare e gestire le risorse in diversi modi, ad esempio in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Ad esempio, puoi utilizzare i tag per: applicare politiche, allocare i costi, distinguere tra le versioni delle risorse o identificare le risorse che supportano determinati requisiti o flussi di lavoro di conformità.

È possibile aggiungere tag ai seguenti tipi di risorse CSPM di Security Hub:

- Regole di automazione
- Policy di configurazione
- Risorsa Hub

Per modificare le chiavi o i valori dei tag per una risorsa CSPM Security Hub, puoi utilizzare l'API CSPM di Security Hub. La console CSPM di Security Hub attualmente non supporta la modifica dei tag.

> **Important**
>
> La modifica dei tag per una risorsa può influire sull'accesso alla risorsa. Prima di modificare un tag per una risorsa, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare i tag per controllare l'accesso alle risorse.

Security Hub CSPM API

Per modificare i tag per una risorsa CSPM (API) di Security Hub

Quando si modifica un tag per una risorsa a livello di codice, si sovrascrive il tag esistente con nuovi valori. Pertanto, il modo migliore per modificare un tag dipende dal fatto che si desideri modificare una chiave di tag, un valore di tag o entrambi. Per modificare una chiave di tag, rimuovi il tag corrente e aggiungi un nuovo tag.

Per modificare o rimuovere solo il valore del tag associato a una chiave di tag, sovrascrivi il valore esistente utilizzando il TagResourcefunzionamento dell'API CSPM di Security Hub. Se utilizzi ilAWS CLI, esegui il comando tag-resource. Nella richiesta, specifica l'Amazon Resource Name (ARN) della risorsa di cui desideri modificare o rimuovere il valore del tag.

Per modificare il valore di un tag, utilizza il `tags` parametro per specificare la chiave del tag di cui desideri modificare il valore del tag. È inoltre necessario specificare il nuovo valore del tag per la chiave. Ad esempio, il AWS CLI comando seguente modifica il valore del tag da `Prod` a `Test` per la chiave di `Environment` tag assegnata alla regola di automazione specificata. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```

Dove:

- `resource-arn`specifica l'ARN della politica di configurazione.
- *`Environment`*è la chiave del tag associata al valore del tag da modificare.
- *`Test`*è il nuovo valore del tag per la chiave di tag specificata (*`Environment`*).

Per rimuovere un valore di tag da una chiave di tag, non specificate un valore per l'`value`argomento della chiave nel `tags` parametro. Esempio:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Se l'operazione ha esito positivo, Security Hub CSPM restituisce una risposta HTTP 200 vuota. Altrimenti, Security Hub CSPM restituisce una risposta HTTP 4 xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Revisione dei tag per le risorse CSPM di Security Hub

Dopo aver aggiunto o modificato i tag per le risorse CSPM di AWS Security Hub, è possibile visualizzare le chiavi e i valori dei tag attualmente presenti in una risorsa. Un tag è un'etichetta che definisci e assegni a una o più AWS risorse, inclusi determinati tipi di risorse Macie. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. Una chiave tag è

un'etichetta generale che funge da categoria per un valore di tag più specifico. Un valore di tag funge da descrittore di una chiave di tag.

I tag consentono di identificare, categorizzare e gestire le risorse in diversi modi, ad esempio in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Ad esempio, puoi utilizzare i tag per: applicare politiche, allocare i costi, distinguere tra le versioni delle risorse o identificare le risorse che supportano determinati requisiti o flussi di lavoro di conformità.

È possibile aggiungere tag ai seguenti tipi di risorse CSPM di Security Hub:

- Regole di automazione
- Policy di configurazione
- Risorsa Hub

È possibile esaminare i tag per una regola di automazione o una politica di configurazione CSPM di Security Hub utilizzando la console CSPM di Security Hub o l'API CSPM di Security Hub. La console non supporta la revisione dei tag per la risorsa. Hub A livello di codice, puoi rivedere i tag per qualsiasi risorsa.

Per esaminare i tag per più risorse CSPM di Security Hub contemporaneamente, utilizza le operazioni di tagging dell'AWS Resource GroupsAPI Tagging.

Console

Per esaminare i tag per una risorsa CSPM Security Hub (console)

1. Utilizzando le credenziali dell'amministratore CSPM di Security Hub, aprire la console CSPM di AWS Security Hub all'indirizzo. https://console.aws.amazon.com/securityhub/
2. A seconda del tipo di risorsa a cui vuoi aggiungere un tag, esegui una delle seguenti operazioni:
   - Per esaminare i tag per una regola di automazione, scegli Automazioni nel riquadro di navigazione. Quindi, scegli una regola di automazione.
   - Per esaminare i tag relativi a una politica di configurazione, scegli Configurazione nel riquadro di navigazione. Quindi, nella scheda Politiche, seleziona l'opzione accanto a una politica di configurazione. Si apre un pannello laterale che mostra il numero di tag assegnati alla politica. Puoi espandere l'intestazione Tags per visualizzare le chiavi e i valori dei tag.

La sezione Tag elenca tutti i tag attualmente assegnati alla risorsa.

Security Hub CSPM API

Per esaminare i tag per una risorsa CSPM (API) Security Hub

Per recuperare e rivedere i tag di una risorsa esistente, richiama l'API. ListTagsForResource Nella tua richiesta, utilizza il `resourceArn` parametro per specificare l'Amazon Resource Name (ARN) della risorsa.

Se utilizzi ilAWS CLI, esegui il comando list-tags-for-resource e usa il parametro `resource-arn` per specificare l'ARN della risorsa. Esempio:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Se l'operazione ha esito positivo, Security Hub CSPM restituisce un array. `tags` Ogni oggetto dell'array specifica un tag (sia la chiave del tag che il valore del tag) attualmente assegnato alla risorsa. Esempio:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Dove `Environment` e `CostCenter` `Owner` sono le chiavi dei tag assegnate alla risorsa. `Prod`è il valore del tag associato alla chiave del `Environment` tag. `12345`è il valore del tag associato alla chiave del `CostCenter` tag. La chiave `Owner` tag non ha un valore di tag associato.

Per recuperare un elenco di tutte le risorse CSPM di Security Hub che dispongono di tag e di tutti i tag assegnati a ciascuna di tali risorse, utilizza il GetResourcesfunzionamento dell'API Tagging. AWS Resource Groups Nella richiesta, imposta il valore del parametro su. `ResourceTypeFilters` `securityhub` A tale scopoAWS CLI, eseguite il comando get-resources e impostate il valore del `resource-type-filters` parametro su. `securityhub` Esempio:

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

Se l'operazione ha esito positivo, Resource Groups restituisce un `ResourceTagMappingList` array. L'array contiene un oggetto per ogni risorsa CSPM Security Hub con tag. Ogni oggetto specifica l'ARN di una risorsa CSPM Security Hub e le chiavi e i valori dei tag assegnati alla risorsa.

Rimuovere i tag dalle risorse CSPM di Security Hub

Se aggiungi tag a una risorsa CSPM di AWS Security Hub, puoi successivamente rimuoverne uno o più. Un tag è un'etichetta che definisci e assegni alle AWS risorse, inclusi alcuni tipi di risorse CSPM di Security Hub. È possibile aggiungere, modificare e rimuovere tag dai seguenti tipi di risorse CSPM di Security Hub: regole di automazione, politiche di configurazione e risorsa. Hub

Per rimuovere i tag da una singola risorsa CSPM AWS di Security Hub, puoi utilizzare l'API CSPM di Security Hub. La console CSPM di Security Hub attualmente non supporta la rimozione dei tag.

Per rimuovere i tag da più risorse CSPM di Security Hub contemporaneamente, utilizza le operazioni di tagging dell'AWS Resource GroupsAPI Tagging.

> **Important**
>
> La rimozione dei tag da una risorsa può influire sull'accesso alla risorsa. Prima di rimuovere un tag, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare il tag per controllare l'accesso alle risorse.

Security Hub CSPM API

Per rimuovere i tag da una risorsa CSPM (API) di Security Hub

Per rimuovere uno o più tag da una risorsa a livello di codice, utilizzate il UntagResourcefunzionamento dell'API CSPM Security Hub. Nella tua richiesta, utilizza il `resourceArn` parametro per specificare l'Amazon Resource Name (ARN) della risorsa da cui rimuovere un tag. Usa il `tagKeys` parametro per specificare la chiave del tag da rimuovere. Per rimuovere più tag, aggiungete il `tagKeys` parametro e l'argomento per ogni tag da rimuovere, separati da una e commerciale (&), ad esempio. `tagKeys=`*`key1`*`&tagKeys=`*`key2` Per rimuovere solo un valore di tag specifico (non una chiave di tag) da una risorsa, modifica il tag anziché rimuovere il tag.

Se utilizzi ilAWS CLI, esegui il comando untag-resource per rimuovere uno o più tag da una risorsa. Per il `resource-arn` parametro, specificate l'ARN della risorsa da cui rimuovere un tag. Utilizzate il `tag-keys` parametro per specificare la chiave del tag da rimuovere. Ad esempio, il comando seguente rimuove il `Environment` tag (sia la chiave del tag che il valore del tag) dalla politica di configurazione specificata:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

Dove `resource-arn` specifica l'ARN della politica di configurazione da cui rimuovere un tag *`Environment`* ed è la chiave del tag da rimuovere.

Per rimuovere più tag da una risorsa, aggiungi ogni chiave di tag aggiuntiva come argomento per il `tag-keys` parametro. Esempio:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

Se l'operazione ha esito positivo, Security Hub CSPM restituisce una risposta HTTP 200 vuota. Altrimenti, Security Hub CSPM restituisce una risposta HTTP 4 xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Quote per Security Hub

Hai Account AWS determinate quote predefinite, precedentemente denominate limiti, per ognuna di esse. Servizio AWS Queste quote rappresentano il numero massimo di risorse o operazioni di servizio per l'account. Questo argomento contiene collegamenti alle quote che si applicano alle risorse e alle operazioni AWS di Security Hub per il tuo account. Salvo diversa indicazione, ogni quota si applica all'account di ciascuno di essiRegione AWS.

Alcune quote possono essere aumentate, mentre altre no. Per richiedere un aumento di una quota, usa la console Service Quotas. Per informazioni su come richiedere un aumento, consulta Richiedere un aumento della quota nella Service Quotas User Guide. Se una quota non è disponibile nella console Service Quotas, utilizza il modulo di aumento del limite di servizio su AWS Support Center Console per richiedere un aumento della quota.

Quote massime

Per un elenco delle quote che si applicano alle risorse del AWS Security Hub, vedere Endpoint e quote del AWS Security Hub nel. Riferimenti generali di AWS

Quote tariffa

Per un elenco delle quote che si applicano alle operazioni dell'API AWS Security Hub, consulta il riferimento all'API AWS Security Hub.

Se si configura l'aggregazione tra regioni in Security Hub CSPM, una chiamata verso `BatchImportFindings` e `BatchUpdateFindings` influisce sulle regioni collegate e sulla regione di aggregazione. L'`GetFindings`operazione recupera i risultati dalle regioni collegate e dalla regione di aggregazione. Tuttavia, le `UpdateStandardsControl` operazioni `BatchEnableStandards` e lo sono. Region-specific

Cronologia dei documenti per AWS Security Hub Guida per l'utente

La tabella seguente descrive le modifiche importanti alla documentazione dall'ultima versione di AWS Security Hub e Security Hub CSPM. Per le versioni dei nuovi controlli CSPM di Security Hub, la data specifica quando i controlli iniziano a essere disponibili nei formati supportati. Regioni AWS Possono essere necessarie 1-2 settimane prima che i controlli siano disponibili in tutte le regioni supportate. Per dettagli sulle modifiche sostanziali ai controlli esistenti, consulta. Registro delle modifiche per i controlli CSPM di Security Hub

Per ricevere notifiche sugli aggiornamenti della AWS Security Hub User Guide, puoi iscriverti a un feed RSS.

Modifica	Descrizione	Data
Nuovo standard di sicurezza	Security Hub CSPM ha rilasciato lo standard CRI Profile v2.2. Questo standard è in linea con il CRI Profile, un framework di sicurezza informatica sviluppato dal Cyber Risk Institute (CRI) che armonizza la sicurezza informatica e le aspettative normative per il settore dei servizi finanziari.	14 ottobre 2026
Le regole di automazione possono aggiornare la criticità delle risorse	Le regole di automazione di Security Hub ora possono aggiornare la criticità delle risorse (regole delle risorse), oltre ad aggiornare i dettagli di ricerca e creare ticket. L'impostazione della criticità delle risorse consente di dare priorità alla correzione in base	1 ottobre 2026

	all'importanza delle risorse interessate per l'azienda.	
Piani di risanamento	Sono stati aggiunti piani di correzione, che raggruppano i risultati relativi all'esposizione per causa principale in modo che un'unica correzione possa risolvere o ridurre la gravità di diverse esposizioni. Per ulteriori informazioni, consulta Piani di riparazione in AWS Security Hub.	30 settembre 2026
Dettagli aggiornati dei risultati informativi sulla scansione della rete	Sono state aggiunte informazioni sui risultati informativi generati da Network Scanning.	3 settembre 2026
Elenco aggiornato delle porte di scansione della rete	È stato aggiunto l'elenco delle porte attualmente supportate da Network Scanning.	18 agosto 2026
Controlli di sicurezza aggiornati	Security Hub CSPM ha rimosso il EFS.6controllo dallo standard AWS Foundational Security Best Practices (FSBP). Questo controllo rimane disponibile negli standard NIST SP 800-53 Rev. 5, NIST SP 800-171 Revision 2 e PCI DSS v4.0.1.	3 agosto 2026
Documentazione avanzata sull'abilitazione del Security Hub	È stata migliorata la guida nella pagina Gestione della configurazione degli account dei membri in un' AWS organizzazione.	7 luglio 2026

Aggiunta la documentazione sulla funzionalità di scansione della rete	Aggiunta documentazione per la funzionalità di scansione della rete di Security Hub	7 luglio 2026
Inventario AI	È stato aggiunto l'inventario AI, che fornisce una visione unificata delle risorse di intelligenza artificiale (AI) e machine learning (ML) gestite e ospitate autonomamente in tutto l' AWS ambiente. Per ulteriori informazioni, consulta l'inventario AI in AWS Security Hub.	7 luglio 2026
Aggiornamenti a una politica gestita: `AWSSecurityHubV2ServiceRolePolicy`	Security Hub ha aggiornato la politica AWS gestita denominata`AWSSecurityHubV2ServiceRolePolicy` . Gli aggiornamenti hanno aggiunto le autorizzazioni per supportare le integrazioni di terze parti, tra cui la gestione di registratori di configurazione di terze parti, la creazione e la gestione dei connettori e l'ottenimento di token di identità Web per la federazione.	30 giugno 2026

Aggiornamenti a una politica gestita: `AWSSecurityHubServiceRolePolicy`	Security Hub CSPM ha aggiornato la policy AWS gestita denominata. `AWSSecurityHubServiceRolePolicy` Gli aggiornamenti hanno aggiunto le autorizzazioni per supportare le integrazioni di terze parti. Questi includono la gestione di registratori di configurazione di terze parti e il recupero delle metriche sullo stato del Connector.	30 giugno 2026
Nuovo standard di sicurezza	Security Hub CSPM ha rilasciato lo standard AI Security Best Practices. Questo standard fornisce un set curato di controlli che rilevano quando le risorse di intelligenza artificiale distribuite non sono in linea con le migliori pratiche di sicurezza.	30 giugno 2026
Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato otto nuovi controlli per lo standard AI Security Best Practices. I nuovi controlli sono: Bedrock.1, BedrockAgentCore.7, SageMaker.20, SageMaker.21, SageMaker.22SageMaker.23SageMaker.24, e. SageMaker.25	30 giugno 2026

Aggiornamenti sul tipo di caratteristiche di impatto e sulla gravità dei risultati dell'esposizione	È stato aggiunto il tipo di caratteristica di impatto ai risultati dell'esposizione. L'impatto descrive il raggio di esplosione potenziale se una risorsa viene compromessa, in base alle autorizzazioni effettive dei principali responsabili associati. AWS Identity and Access Management È stato aggiornato il calcolo della gravità per utilizzare una matrice di rischio di verosimiglianza e impatto in linea con le linee guida del NIST. È stata aggiunta una guida alla correzione per risorsa per le caratteristiche del percorso di accesso all'impatto.	23 giugno 2026
Aggiornamenti agli standard e ai controlli di sicurezza	Abbiamo eliminato i RDS.18 controlli ECS.1 and e li abbiamo rimossi da tutti gli standard applicabili. Da quando la EC2-Classic rete Amazon è stata ritirata, le istanze di Amazon Relational Database Service (Amazon RDS) non possono più essere distribuite al di fuori di un VPC.	5 giugno 2026

Aggiornamenti per il registratore collegato al servizio CSPM	Sono state aggiunte informazioni relative al nuovo registratore di configurazione collegato al servizio che consente a Security Hub CSPM di eseguire controlli di sicurezza in base alle informazioni di configurazione delle risorse.	27 maggio 2026
Risultati di accesso non utilizzati	Security Hub ha aggiunto funzionalità per generare e visualizzare i risultati degli accessi non utilizzati da IAM Access Analyzer Comprensione dei risultati di accesso non utilizzati in Security Hub	19 maggio 2026
Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato cinque nuovi controlli . Alcuni controlli supportano lo standard AWS Foundational Security Best Practices (FSBP). La maggior parte dei controlli supporta i requisiti NIST SP 800-53 Rev. 5. • Per lo standard AWS FSBP, gli ID per i controlli applicabili sono: e. BedrockAgentCore.5BedrockAgentCore.6 • Per NIST SP 800-53 Rev. 5, gli ID per i controlli applicabili sono:,, e. BedrockAgentCore.3BedrockAgentCore.4SageMaker.18	15 maggio 2026

Aggiornamenti a una politica gestita: `AWSSecurityHubServiceRolePolicy`	Security Hub CSPM ha aggiornato la policy AWS gestita denominata. `AWSSecurityHubServiceRolePolicy` Gli aggiornamenti hanno aggiunto le autorizzazioni per gestire i registratori di configurazione collegati al servizio Security Hub CSPM e creare il ruolo collegato al servizio. AWS Config	29 aprile 2026
Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato quattro nuovi controlli per lo standard AWS Foundational Security Best Practices (FSBP). I nuovi controlli sono: BedrockAgentCore.1,, e. BedrockAgentCore.2RDS.51SageMaker.19	22 aprile 2026
Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato cinque nuovi controlli per lo standard AWS Foundational Security Best Practices (FSBP). I nuovi controlli sono: APIGateway.11,,, e EC2.183. EKS.9SageMaker.16SageMaker.17	7 aprile 2026

Aggiornamenti agli standard e ai controlli di sicurezza	Abbiamo eliminato i AppSync.6 controlli AppSync.1 and e li abbiamo rimossi dallo standard AWS Foundational Security Best Practices (FSBP). AWS AppSync ora fornisce la crittografia predefinita su tutte le cache API attuali e future.	9 marzo 2026
Aggiornamenti agli standard e ai controlli di sicurezza	Abbiamo ritirato il ECS.1 controllo e rimosso il controllo dallo standard AWS Foundational Security Best Practices (FSBP) e dallo standard NIST SP 800-53 Rev. 5.	4 marzo 2026
Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato undici nuovi controlli per lo standard AWS Foundational Security Best Practices (FSBP). I nuovi controlli sono: APIGateway.10,,,, e ELB.21. ELB.22RDS.50SageMaker.9SageMaker.10SageMaker.11SageMaker.12SageMaker.13SageMaker.14SageMaker.15	16 febbraio 2026

Aggiornamenti agli standard e ai controlli di sicurezza	Abbiamo ritirato il MQ.3 controllo e rimosso il controllo da tutti gli standard applicabili. Abbiamo ritirato il controllo a causa dei requisiti di Amazon MQ per gli aggiornamenti automatici delle versioni secondarie. In precedenza, questo controllo si applicava allo standard AWS Foundational Security Best Practices (FSBP), allo standardNIST SP 800-53 Rev. 5 e allo standard PCI DSS v4.0.1.	12 gennaio 2026
Aggiornamenti alla documentazione relativa alla stima dei costi	Sono stati aggiunti dettagli alla documentazione dello strumento di stima dei costi di Security Hub su come concedere l'accesso a più account per effettuare stime in account diversi dall'account di gestione.	12 gennaio 2026
Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato cinque nuovi controlli per lo standard AWS Foundational Security Best Practices (FSBP). I nuovi controlli sono: CloudFormation.4,,, e CloudFront.17. ECS.19ECS.20ECS.21	6 gennaio 2026

Aggiornamenti agli standard e ai controlli di sicurezza	A causa dei requisiti di Amazon MQ per gli aggiornamenti automatici delle versioni secondarie, abbiamo intenzione di ritirare MQ.3 e rimuovere il controllo da tutti gli standard applicabili il 12 gennaio 2026. Attualmente, il controllo si applica allo standard AWS Foundational Security Best Practices (FSBP), allo standardNIST SP 800-53 Rev. 5 e allo standard PCI DSS v4.0.1.	12 dicembre 2025
Contenuto aggiornato per Service-Managed Standard: AWS Control Tower	Contenuto aggiornato per Service-Managed Standard: per AWS Control Tower fornire una guida migliore per la creazione, la visualizzazione e la disabilitazione dei controlli nel modulo standard. AWS Control Tower	8 dicembre 2025
Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato sette nuovi controlli per lo standard AWS Foundational Security Best Practices (FSBP). I nuovi controlli sono: Cognito.4 ,,, Cognito.5Cognito.6 , EC2.182e. CloudFormation.3ECS.18SES.3	8 dicembre 2025

Contenuti aggiornati per la disponibilità generale di Security Hub	Contenuti aggiunti per supportare la versione General Availability di AWS Security Hub	2 dicembre 2025
Contenuti aggiornati per Security Hub	Contenuti aggiunti per Trends e Region Aggregation. Queste modifiche supportano la versione di anteprima di Security Hub.	21 novembre 2025
Aggiornamenti a una politica gestita: `AWSSecurityHubV2ServiceRolePolicy`	Security Hub ha aggiornato la politica AWS gestita denominata`AWSSecurityHubV2ServiceRolePolicy` . Gli aggiornamenti hanno aggiunto funzionalità di misurazione per Amazon Elastic Container Registry AWS Lambda CloudWatch, Amazon e AWS Identity and Access Management per supportare le funzionalità di Security Hub. Gli aggiornamenti hanno anche aggiunto il supporto per i AWS Config registratori globali. Queste modifiche supportano la versione di anteprima di Security Hub.	17 novembre 2025

Aggiornamenti a una politica gestita: AWSSecurityHubOrganizationsAccess	Security Hub ha aggiornato la politica AWS gestita denominata AWSSecurityHubOrganizationsAccess . Gli aggiornamenti hanno aggiunto le autorizzazioni per descrivere le politiche delle risorse che supportano le funzionalità di Security Hub. Queste modifiche supportano la versione di anteprima di Security Hub.	17 novembre 2025
Aggiornamenti a una politica gestita: AWSSecurityHubFullAccess	Security Hub ha aggiornato la politica AWS gestita denominata AWSSecurityHubFullAccess . Gli aggiornamenti hanno aggiunto funzionalità di gestione GuardDuty, Amazon Inspector e gestione degli account per supportare le funzionalità di Security Hub. Queste modifiche supportano la versione di anteprima di Security Hub.	17 novembre 2025

Aggiornamenti ai controlli di sicurezza	Abbiamo modificato la gravità di 10 controlli CSPM di Security Hub: CloudFront.7, CloudTrail.5, ELB.7, GuardDuty.7, MQ.3, Opensearch.10,, RDS.7 ServiceCatalog.1 SNS.4, e. SQS.3 Per un'analisi dettaglia ta delle modifiche, consulta il registro delle modifiche per i controlli CSPM di Security Hub.	13 novembre 2025
Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato sei nuovi controlli per lo standard AWS Foundational Security Best Practices (FSBP). I nuovi controlli sono: Cognito.3 ,,, DMS.13, EC2.181e. RDS.43RDS.47RDS.48	28 ottobre 2025
Nuovo standard di sicurezza	Security Hub CSPM ora fornisce uno standard di sicurezza in linea con CIS Foundations Benchmark v5.0.0. AWS Questo nuovo standard include 40 controlli di sicurezza esistenti. I controlli eseguono controlli automatic i che valutano la conformit à di determinate risorse a un sottoinsieme dei requisiti definiti dal framework.	16 ottobre 2025

Nuova integrazione di terze parti	Elasticè una nuova integrazione di terze parti che può ricevere risultati da Security Hub CSPM.	3 ottobre 2025
Aggiornamenti agli standard e ai controlli di sicurezza	Abbiamo eliminato i RedshiftServerless.7 controlli Redshift.9 and e li abbiamo rimossi da tutti gli standard applicabili. Abbiamo eliminato questi controlli a causa delle limitazioni intrinseche di Amazon Redshift che impedivano l'efficace correzione dei risultati dei `FAILED` controlli. In precedenza, questi controlli si applicavano allo standard AWS Foundational Security Best Practices (FSBP) e allo standard NIST SP 800-53 Rev. 5. Il Redshift.9 controllo si applicava anche allo standard gestito dai servizi.AWS Control Tower	24 settembre 2025
Disponibilità regionale	Security Hub CSPM è ora disponibile nella regione Asia Pacifico (Nuova Zelanda). Per un elenco completo delle aree Regioni AWS in cui Security Hub CSPM è attualmente disponibile, consulta Endpoint e quote AWS di Security Hub nel. Riferimenti generali di AWS	19 settembre 2025

Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato due nuovi controlli per lo standard AWS Foundational Security Best Practices (FSBP): e. CloudFront.16RDS.46	3 settembre 2025
Disponibilità regionale	Lo standard AWS Resource Tagging è ora disponibile nelle regioni Asia Pacifico (Tailandia) e Messico (Centrale).	29 agosto 2025
Aggiornamenti agli standard e ai controlli di sicurezza	A causa delle limitazioni di Amazon Redshift, abbiamo intenzione di ritirare i RedshiftServerless.7 controlli Redshift.9 and e di rimuoverli da tutti gli standard applicabili il 15 settembre 2025. Attualmente, questi controlli si applicano allo standard AWS Foundational Security Best Practices (FSBP) e allo standard NIST SP 800-53 Rev. 5. Il Redshift.9 controllo si applica anche allo standard gestito dai servizi.AWS Control Tower	15 agosto 2025

Nuovo oggetto per i dettagli delle risorse nell'ASFF	Il AWS Security Finding Format (ASFF) ora include un oggetto `CodeRepository` risorsa. Questo oggetto fornisce dettagli su un repository di codice esterno collegato alle AWS risorse e configurato Amazon Inspector per la scansione delle vulnerabilità.	1 agosto 2025
Disponibilità regionale	Security Hub CSPM è ora disponibile nella regione Asia Pacifico (Taipei). Per un elenco completo delle aree Regioni AWS in cui Security Hub CSPM è attualmente disponibile, consulta Endpoint e quote AWS di Security Hub nel. Riferimenti generali di AWS	23 luglio 2025
Nuova integrazione di terze parti	Dynatraceè una nuova integrazione di terze parti che può ricevere risultati da Security Hub CSPM.	18 luglio 2025

Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato 13 nuovi controlli. La maggior parte dei controlli supporta lo standard AWS Foundational Security Best Practices (FSBP). Alcuni controlli supportano i requisiti NIST SP 800-53 Rev. 5. • Per lo standard AWS FSBP, gli ID per i controlli applicabili sono: CloudFront.15,,,, Cognito.2, EC2.180, ELB.18, MSK.4, MSK.5MSK.6, RDS.45e. Redshift. 18S3.25SSM.6SSM.7 • Per NIST SP 800-53 Rev. 5, gli ID per i controlli applicabili sono: e. Lambda.7RDS.45	15 luglio 2025
Aggiornamenti alla generazione dei risultati del controllo	Per aiutarti a tenere traccia delle modifiche alla conformità, Security Hub CSPM ora aggiorna i risultati di controllo esistenti, anziché generarne di nuovi, in caso di modifiche allo stato di conformità delle singole risorse. Ciò significa che è possibile utilizzare i dati forniti dai singoli risultati per tenere traccia delle modifiche di conformità per particolari risorse rispetto a controlli particolari.	3 luglio 2025

Aggiornamenti agli standard e ai controlli di sicurezza	Abbiamo rimosso il IAM.13controllo dallo standard PCI DSS v4.0.1. Abbiamo anche rimosso il IAM.17controllo dallo standard NIST SP 800-171 Revision 2. Gli standard non richiedono esplicitamente i controlli forniti da questi controlli. Abbiamo inoltre aggiornato i dettagli relativi ai requisiti relativi a questi standard per determinati controlli che controllano le politiche sulle password di IAM: IAM.7 e IAM.10 attraverso IAM.17.	30 giugno 2025
Aggiornamenti relativi alla conservazione dei risultati	Security Hub CSPM ora archivia i risultati archiviati per 30 giorni anziché 90 giorni, il che può ridurre il rumore delle ricerche. Per una conservazione a lungo termine, puoi esportare i risultati in un bucket S3 utilizzando un'azione personalizzata con una regola Amazon. EventBridge	20 giugno 2025

Aggiornamenti alle politiche gestite esistenti	Security Hub CSPM ha aggiunto una nuova autorizzazione alla policy AWS gestita denominata. `AWSSecurityHubOrganizationsAccess` L'autorizzazione consente alla direzione dell'organizzazione di abilitare e gestire Security Hub e Security Hub CSPM all'interno di un'organizzazione. Security Hub CSPM ha inoltre aggiunto nuove autorizzazioni alla policy AWS gestita denominata. `AWSSecurityHubFullAccess` L'autorizzazione consente ai responsabili di creare un ruolo collegato al servizio per Security Hub.	18 giugno 2025
Versione di anteprima pubblica e una nuova politica gestita per Security Hub	Versione di anteprima pubblica di AWS Security Hub e della AWS Security Hub User Guide. Questa versione include una nuova politica AWS gestita,`AWSSecurityHubV2ServiceRolePolicy` . La policy consente a Security Hub di gestire AWS Config le regole e le risorse del Security Hub nell'organizzazione di un cliente e per conto del cliente. Security Hub è in versione di anteprima ed è soggetto a modifiche.	17 giugno 2025

Aggiornamenti agli standard e ai controlli di sicurezza	Abbiamo rimosso il IAM.10controllo dallo standard PCI DSS v4.0.1. Questo controllo verifica se le politiche relative alle password degli account per gli utenti IAM soddisfano i requisiti minimi, inclusa una lunghezza minima della password di 7 caratteri. PCI DSS v4.0.1 ora richiede che le password abbiano un minimo di 8 caratteri. Il IAM.10 controllo continua ad applicarsi allo standard PCI DSS v3.2.1, che ha requisiti di password diversi.	30 maggio 2025
Nuovo standard di sicurezza	Security Hub CSPM ora fornisce uno standard di sicurezza che si allinea al framework di sicurezza informatica e conformità NIST SP 800-171 Revisione 2. Questo nuovo standard include più di 60 controlli di sicurezza esistenti. I controlli eseguono controlli automatici che valutano la conformità di determinate Servizi AWS risorse a un sottoinsieme dei requisiti definiti dal framework.	29 maggio 2025

Aggiornamenti ai controlli di sicurezza	Security Hub CSPM ha ripristinato in tutto il rilascio del seguente controllo Regioni AWS: [RDS.46] Le istanze DB RDS non devono essere distribuite in sottoreti pubbliche con percorsi verso i gateway Internet. In precedenza, questo controllo supportava lo standard AWS Foundatio nal Security Best Practices (FSBP).	8 maggio 2025

Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato 9 nuovi controlli. La maggior parte dei controlli supporta lo standard AWS Foundational Security Best Practices (FSBP). Alcuni controlli supportano i requisiti NIST SP 800-53 Rev. 5. • Per lo standard AWS FSBP, gli ID per i controlli applicabili sono: DocumentDB.6,,,, RDS.44RedshiftServerless .2RedshiftServerless .3RedshiftServerless .5RedshiftServerless.6, e (successivamente ritirati). RedshiftServerless.7 • Per NIST SP 800-53 Rev. 5, gli ID per i controlli applicabili sono: CloudTrail.10, RedshiftServerless.4e (successivamente ritirati). RedshiftServerless.7	07 maggio 2025

Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato 24 nuovi controlli. La maggior parte dei controlli supporta lo standard AWS Foundational Security Best Practices (FSBP) o Resource Tagging.AWS Alcuni controlli supportano i requisiti NIST SP 800-53 Rev. 5. • Per lo standard AWS FSBP, gli ID per i controlli applicabili sono:,, e. EC2.173RDS.41RDS.42SageMaker.8 • Per lo standard AWS Resource Tagging, gli ID per i controlli applicabili sono: Amplify.1Amplify.2 Batch.4DataSync.2EC2.174, EC2.175, EC2.176, EC2.177, EC2.178, EC2.179, Redshift.17, SageMaker.6, SageMaker.7, SSM.5, Transfer.4Transfer.5Transfer.6 e. Transfer.7 • Per NIST SP 800-53 Rev. 5, gli ID per i controlli applicabili sono: e. ECS.17RDS.42	16 aprile 2025

Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato quattro nuovi controlli per lo standard AWS Foundational Security Best Practices. I controlli sono: • the section called "[FSx.3] I file system FSx for OpenZFS devono essere configurati per la distribuzione Multi-AZ" • the section called "[FSx.4] I file system FSx for NetApp ONTAP devono essere configurati per l'implementazione Multi-AZ" • the section called "[FSx.5] I file system FSx for Windows File Server devono essere configurati Multi-AZ per la distribuzione" • the section called "[RedshiftServerless.1] I gruppi di lavoro Serverless di Amazon Redshift devono utilizzare un routing VPC avanzato"	18 marzo 2025

Aggiornamenti agli standard e ai controlli di sicurezza	Abbiamo rimosso il controllo RDS.18 di sicurezza (in seguito ritirato) dallo standard AWS Foundational Security Best Practices e i controlli automatici per i requisiti NIST SP 800-53 Rev. 5. Da quando la EC2-Classic rete Amazon è stata ritirata, le istanze di Amazon Relational Database Service (Amazon RDS) non possono più essere distribuite al di fuori di un VPC.	7 marzo 2025
Aggiornamenti per controllare i risultati	Security Hub CSPM ora genera `WARNING` i risultati per un controllo abilitato se la registrazione delle risorse non è attivata AWS Config per il tipo di risorsa controllata dal controllo. Questo può aiutarti a identificare e risolvere potenziali lacune di configura zione nei controlli di sicurezza.	25 febbraio 2025

Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato 11 nuovi controlli. I controlli sono: • the section called "[Connect .2] Le istanze Connect Customer devono avere la CloudWatch registrazione abilitata" • the section called "[ECR.5] I repository ECR devono essere crittografati e gestiti dal cliente AWS KMS keys" • the section called "[ELB.17] Gli Application and Network Load Balancer con listener devono utilizzare le politiche di sicurezza consigliate" • the section called "[Glue.4] AWS Glue I job Spark devono essere eseguiti su versioni supportate di AWS Glue" • the section called "[GuardDuty.11] Il monitoraggio del GuardDuty runtime deve essere abilitato" • the section called "[GuardDuty.12] Il monitoraggio del runtime GuardDuty ECS deve essere abilitato" • the section called "[GuardDuty.13] Il monitoraggio del runtime GuardDuty EC2 deve essere abilitato"	24 febbraio 2025

- the section called "[Network Firewall.10] I firewall Network Firewall devono avere la protezione da cambio di sottorete abilitata"
- the section called "[RDS.40] Le istanze DB di RDS per SQL Server devono pubblicare i log in Logs CloudWatch"
- the section called "[SQS.3] Le politiche di accesso alla coda di SQS non dovrebbero consentire l'accesso pubblico"
- the section called "[Transfer.3] I connettori Transfer Family dovrebbero avere la registrazione abilitata"

Nuovi controlli di sicurezza	Security Hub CSPM ha rilasciato 37 nuovi controlli per il AWS Resource Tagging Standard. Security Hub CSPM ha inoltre rilasciato i seguenti nuovi controlli: • the section called "[EMR.3] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate a riposo" • the section called "[EMR.4] Le configurazioni di sicurezza di Amazon EMR devono essere crittografate in transito" • the section called "[SageMaker.5] SageMaker i modelli dovrebbero avere l'isolamento della rete abilitato"	22 gennaio 2025
Nuovo controllo di sicurezza	Security Hub CSPM ha rilasciato le impostazioni VPC Block Public Access di EC2.172 EC2 che dovrebbero bloccare il traffico del gateway Internet.	15 gennaio 2025

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub. • the section called "[Cognito .1] I pool di utenti di Cognito dovrebbero avere la protezione dalle minacce attivata con la modalità di imposizione completa delle funzioni per l'autenticazione standard" • the section called "[RDS.38] Le istanze DB RDS per PostgreSQL devono essere crittografate in transito" • the section called "[RDS.39] Le istanze DB RDS per MySQL devono essere crittografate in transito" • the section called "[Redshif t.16] I gruppi di sottoreti del cluster Redshift devono avere sottoreti provenienti da più zone di disponibilità"	17 dicembre 2024
Security Hub CSPM supporta PCI DSS v4.0.1	Security Hub CSPM ora supporta la versione 4.0.1 del Payment Card Industry Data Security Standard (PCI DSS). Per ulteriori informazioni sullo standard e sui controlli ad esso applicabili, vedere PCI DSS in Security Hub CSPM.	11 dicembre 2024

Security Hub CSPM riceve i risultati della sequenza di GuardDuty attacco	Security Hub CSPM ora riceve i risultati della sequenza di attacco da Amazon GuardDuty Extended Threat Detection. I dettagli relativi alla ricerca della sequenza di attacco sono disponibili nell'oggetto di rilevamento del AWS Security Finding Format (ASFF).	1 dicembre 2024
Security Hub CSPM supportato nella nuova versione Regione AWS	Security Hub CSPM è ora disponibile nella regione Asia Pacifico (Malesia). Alcuni controlli di sicurezza hanno limitazioni regionali . Per un elenco dei controlli che non sono disponibili in questa regione, consulta Limiti regionali sui controlli CSPM di Security Hub.	22 novembre 2024
Modifiche a Config.1	Security Hub CSPM ha aumentato la severità del Config.1 controllo da `MEDIUM` a `CRITICAL` e ha aggiunto nuovi codici di stato e motivi di stato per i risultati non riusciti Config.1 . Per ulteriori informazioni sulle modifiche, vedere la voce relativa al 20 novembre 2024 nel registro delle modifiche per i controlli CSPM di Security Hub.	20 novembre 2024

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub. Questi controlli fanno parte di AWS Foundatio nal Security Best Practices e NIST SP 800-53 Rev. 5 e valutano se un cloud privato virtuale (VPC) che gestisci ha un endpoint VPC di interfacc ia per una risorsa or. Servizio AWS AWS • the section called "[EC2.55] I VPC devono essere configurati con un endpoint di interfaccia per l'API ECR" • the section called "[EC2.56] I VPC devono essere configurati con un endpoint di interfaccia per Docker Registry" • the section called "[EC2.57] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager" • the section called "[EC2.58] I VPC devono essere configurati con un endpoint di interfaccia per Systems Manager Incident Manager Contacts" • the section called "[EC2.60] I VPC devono essere configurati con un endpoint	15 novembre 2024

di interfaccia per Systems Manager Incident Manager"

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub. • [AppSync.1] Le cache AWS AppSync delle API devono essere crittografate quando sono inattive • [AppSync.6] Le cache AWS AppSync delle API devono essere crittografate in transito • the section called "[EC2.170] I modelli di avvio EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)" • the section called "[EC2.171] Le connessioni VPN EC2 devono avere la registrazione abilitata" • the section called "[EFS.8] I file system EFS devono essere crittografati quando sono inattivi" • the section called "[KMS.5] Le chiavi KMS non devono essere accessibili al pubblico" • the section called "[SNS.4] Le politiche di accesso agli argomenti SNS non dovrebbero consentire l'accesso pubblico"	18 ottobre 2024

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub. • the section called "[ECS.16] I set di attività ECS non devono assegnare automaticamente indirizzi IP pubblici" • the section called "[GuardDuty.7] GuardDuty EKS Runtime Monitoring deve essere abilitato" • the section called "[Kinesis.3] I flussi Kinesis devono avere un periodo di conservazione dei dati adeguato" • the section called "[MSK.3] I connettori MSK Connect devono essere crittografati in transito" • the section called "[RDS.36] Le istanze DB di RDS per PostgreSQL devono pubblicare i log in Logs CloudWatch" • the section called "[RDS.37] I cluster Aurora PostgreSQL DB devono pubblicare i log in Logs CloudWatch" • the section called "[S3.24] I punti di accesso S3 Multi-Region devono avere le impostazioni di blocco	3 ottobre 2024

dell'accesso pubblico abilitate"

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub. • the section called "[Athena.4] I gruppi di lavoro Athena dovrebbero avere la registrazione abilitata" • the section called "[CodeBuild.7] le esportazioni dei gruppi di CodeBuild report devono essere crittografate quando sono inattive" • the section called "[DataSync.1] DataSync le attività dovrebbero avere la registrazione abilitata" • the section called "[EFS.7] I file system EFS devono avere i backup automatici abilitati" • Glue.2 (ritirato) • the section called "[Glue.3] AWS Glue le trasformazioni di apprendimento automatico devono essere crittografate quando sono inutilizzate" • the section called "[WorkSpaces.1] i volumi WorkSpaces utente devono essere crittografati quando sono inattivi" • the section called "[WorkSpaces.2] i volumi WorkSpaces	30 agosto 2024

	root devono essere crittografati quando sono inattivi"	
Nuovo pannello di ricerca	Il nuovo pannello di ricerca sulla console CSPM di Security Hub ti aiuta ad agire rapidamente sui risultati, rivedere i dettagli delle risorse e la cronologia dei risultati e trovare altre informazioni pertinenti su un risultato.	16 agosto 2024
Aggiornamento al controllo Config.1	Il Config.1controllo verifica se AWS Config è abilitato, utilizza il ruolo collegato al servizio e registra le risorse per i controlli abilitati. Security Hub CSPM ha aggiunto un parametro di controllo personalizzato denominato. `includeConfigServiceLinkedRoleCheck` Impostando questo parametro su`false`, è possibile scegliere di non verificare se AWS Config utilizza il ruolo collegato al servizio.	15 agosto 2024
Designare una regione d'origine senza regioni collegate	Ora puoi creare un aggregatore di ricerca e stabilire una regione d'origine senza collegarne nessuna Regioni AWS alla regione d'origine . Ciò consente di abilitare la configurazione centrale senza specificare le regioni collegate.	25 luglio 2024

Seleziona i controlli disponibili in più regioni	I seguenti controlli sono ora disponibili in aggiunta Regioni AWS, tra cui Stati Uniti orientali (Virginia settentrionale) e Stati Uniti orientali (Ohio). • the section called "[DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi" • the section called "[DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata" • the section called "[DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato" • the section called "[DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato" • the section called "[DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito" • the section called "[EFS.6] I target di montaggio EFS non devono essere associati	15 luglio 2024

a sottoreti che assegnano indirizzi IP pubblici all'avvio"

- [EKS.3] I cluster EKS devono utilizzare segreti Kubernetes crittografati
- the section called "[FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup"
- the section called "[MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch"
- [MQ.3] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie
- the section called "[Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati"
- the section called "[Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate"
- the section called "[SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1"
- the section called "[Service Catalog.1] I portafogli

Service Catalog devono essere condivisi all'interno di un AWS solo organizzazione"

- the section called "[Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint"

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub: • the section called "[GuardDuty.5] GuardDuty EKS Audit Log Monitoring deve essere abilitato" • the section called "[GuardDuty.6] La protezione GuardDuty Lambda deve essere abilitata" • the section called "[GuardDuty.8] La protezione GuardDuty da malware per EC2 deve essere abilitata" • the section called "[GuardDuty.9] La protezione GuardDuty RDS deve essere abilitata" • the section called "[GuardDuty.10] La protezione GuardDuty S3 deve essere abilitata" • the section called "[Inspector.1] La scansione di Amazon Inspector EC2 deve essere abilitata" • the section called "[Inspector.2] La scansione ECR di Amazon Inspector deve essere abilitata" • the section called "[Inspector.3] La scansione del codice Amazon Inspector	11 luglio 2024

Lambda deve essere abilitata"

- the section called "[Inspector.4] La scansione standard di Amazon Inspector Lambda deve essere abilitata"

Rilascio di CIS AWS Foundations Benchmark v3.0.0	Security Hub CSPM ha rilasciato Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0. La versione include i seguenti nuovi controlli, oltre a mappature su diversi controlli esistenti. • the section called "[EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'ingresso da 0.0.0. 0/0 alle porte di amministrazione del server remoto" • the section called "[EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server" • the section called "[IAM.26] SSL/TLS I certificati scaduti gestiti in IAM devono essere rimossi" • the section called "[IAM.27] Le identità IAM non devono avere la AWSCloudShellFullAccess policy allegata" • the section called "[IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato"	13 maggio 2024

- the section called "[S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto"
- the section called "[S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto"

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub: • the section called "[DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi" • the section called "[DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata" • the section called "[DMS.11] Gli endpoint DMS per MongoDB dovrebbero avere un meccanismo di autenticazione abilitato" • the section called "[DMS.12] Gli endpoint DMS per Redis OSS devono avere TLS abilitato" • the section called "[DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito" • the section called "[EFS.6] I target di montaggio EFS non devono essere associati a sottoreti che assegnano indirizzi IP pubblici all'avvio"	3 maggio 2024

- [EKS.3] I cluster EKS devono utilizzare segreti Kubernetes crittografati
- the section called "[FSx.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup"
- the section called "[MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch"
- [MQ.3] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie
- the section called "[Opensearch.11] OpenSearch i domini devono avere almeno tre nodi primari dedicati"
- the section called "[Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate"
- the section called "[SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1"
- the section called "[Service Catalog.1] I portafogli Service Catalog devono essere condivisi all'interno

	di un AWS solo organizza zione" • the section called "[Transfe r.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint"	
AWS Standard di etichettatura delle risorse	Il AWS Resource Tagging Standard di Security Hub CSPM è ora disponibile a tutti, insieme ai nuovi controlli che si applicano allo standard.	30 aprile 2024
Aggiornamento alla politica gestita esistente	Security Hub CSPM ha aggiornato la politica AWS gestita denominata `AmazonSecurityHubF ullAccess` per ottenere dettagli sui prezzi dei prodotti Servizi AWS e dei prodotti.	24 aprile 2024
In-context configurazione dei parametri di controllo	Se utilizzi la configurazione centrale, ora puoi configura re i parametri di controllo nel contesto, dalla pagina dei dettagli di un controllo sulla console CSPM di Security Hub.	29 marzo 2024
Aggiornamento alla politica gestita esistente	Security Hub CSPM ha aggiornato la policy AWS gestita denominata `AWSSecurityHubRead OnlyAccess` aggiungendo un `Sid` campo.	22 febbraio 2024

Nuovo controllo di sicurezza	Il controllo [Macie.2] Il rilevamento automatico dei dati sensibili di Macie dovrebbe essere abilitato è ora disponibile. Per i limiti regionali relativi a questo controllo, vedi Disponibilità dei controlli per regione.	19 febbraio 2024
Security Hub CSPM disponibile in Canada occidentale (Calgary)	Security Hub CSPM è ora disponibile in Canada occidentale (Calgary). Tutte le funzionalità CSPM di Security Hub sono ora disponibili in questa regione, ad eccezione di alcuni controlli di sicurezza . Per ulteriori informazioni, vedere Disponibilità dei controlli per regione.	20 dicembre 2023

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub: • the section called "[Backup.1] AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi" • the section called "[DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata" • the section called "[EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata" • the section called "[EKS.8] I cluster EKS dovrebbero avere la registrazione di controllo abilitata" • the section called "[EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata" • the section called "[FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi"	14 dicembre 2023

- the section called "[Macie.1] Amazon Macie dovrebbe essere abilitato"
- the section called "[MSK.2] I cluster MSK dovrebbero avere configurato un monitoraggio avanzato"
- the section called "[Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità"
- the section called "[Network Firewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità"
- the section called "[Network Firewall.2] La registrazione del Network Firewall deve essere abilitata"
- the section called "[Opensearch.10] OpenSearch sui domini dovrebbe essere installato l'ultimo aggiornamento software"
- the section called "[PCA.1] AWS Private CA l'autorità di certificazione principale deve essere disabilitata"
- the section called "[S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate"

	• the section called "[S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata"	
Alla ricerca di un arricchimento	Security Hub CSPM ha aggiunto i nuovi campi `AwsAccountName` di ricerca e `ApplicationName` al AWS Security Finding Format (ASFF). `ApplicationArn`	27 novembre 2023
Miglioramenti alla dashboard di riepilogo	Ora puoi accedere a più widget del dashboard nella pagina di riepilogo della console Security Hub CSPM, salvare i set di filtri del dashboard per concentrarti rapidamente su problemi di sicurezza specifici e personalizzare il layout del dashboard.	27 novembre 2023
Configurazione centrale	La configurazione centrale è ora disponibile. Con la configurazione centrale, l'amministratore delegato CSPM di Security Hub può configurare CSPM, standard e controlli di Security Hub su più account dell'organizzazione, unità organizzative (OU) e regioni.	27 novembre 2023

Aggiornamenti alla policy gestita	Security Hub CSPM ha aggiunto nuove autorizzazioni alla policy `AWSSecurityHubServiceRolePolicy` gestita che consentono a Security Hub CSPM di leggere e aggiornare le proprietà di controllo di sicurezza personalizzabili.	26 novembre 2023
Parametri di controllo personalizzati	È ora possibile personalizzare i valori dei parametri per determinati controlli CSPM di Security Hub. Ciò può rendere i risultati relativi a un controllo specifico più pertinenti ai requisiti aziendali e alle aspettative di sicurezza.	26 novembre 2023
Aggiornamenti alle politiche gestite	Security Hub CSPM ha aggiornato `AWSSecurityHubFullAccess` e `AWSSecurityHubOrganizationsAccess` gestito le politiche che consentono di utilizzare, rispettivamente, le funzionalità CSPM di Security Hub e l'integrazione con. AWS Organizations	16 novembre 2023

Controlli di sicurezza esistenti aggiunti a Standard: Service-Managed AWS Control Tower	I seguenti controlli CSPM di Security Hub esistenti sono stati aggiunti a Service-Managed Standard:. 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 novembre 2023

Aggiornamenti alla policy gestita	Security Hub CSPM ha aggiunto una nuova autorizzazione di etichettatura alla politica `AWSSecurityHubServiceRolePolicy` gestita che consente a Security Hub CSPM di leggere i tag delle risorse relativi ai risultati.	7 novembre 2023

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub: • the section called "[AppSync.5] AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API" • the section called "[DMS.6] L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato" • the section called "[DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata" • the section called "[DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata" • the section called "[DMS.9] Gli endpoint DMS devono utilizzare SSL" • the section called "[DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche" • the section called "[DocumentDB.4] I cluster	10 ottobre 2023

Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch"

- the section called "[DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata"
- the section called "[ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione"
- the section called "[EventBridge.3] i bus di eventi EventBridge personalizzati dovrebbero avere una politica basata sulle risorse allegata"
- the section called "[EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata"
- the section called "[MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker"
- the section called "[MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione active/standby"
- the section called "[MQ.6] I broker RabbitMQ dovrebber

o utilizzare la modalità di distribuzione del cluster"

- the section called "[Network Firewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata"
- the section called "[RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch"
- the section called "[] RDS.35 I cluster RDS DB devono avere l'aggiornamento automatico delle versioni secondarie abilitato"
- the section called "[Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS"
- the section called "[WAF.12] AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch"

Aggiornamenti alla policy gestita	Security Hub CSPM ha aggiunto nuove azioni Organizations alla policy `AWSSecurityHubServiceRolePolicy` gestita che consentono a Security Hub CSPM di recuperare informazioni su account e unità organizzative (OU). Abbiamo anche aggiunto nuove azioni CSPM di Security Hub che consentono a Security Hub CSPM di leggere e aggiornare le configurazioni dei servizi, inclusi standard e controlli.	27 settembre 2023

Controlli di sicurezza esistenti aggiunti a Standard: Service-Managed AWS Control Tower	I seguenti controlli CSPM di Security Hub esistenti sono stati aggiunti a Service-Managed Standard:. AWS Control Tower • [Athena.1] I gruppi di lavoro Athena devono essere crittografati quando sono inattivi • the section called "[DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi" • the section called "[DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato" • the section called "[Neptune.1] I cluster Neptune DB devono essere crittografati quando sono inattivi" • the section called "[Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch" • the section called "[Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche"	26 settembre 2023

- the section called "[Neptune .4] I cluster Neptune DB dovrebbero avere la protezione da eliminazione abilitata"
- the section called "[Neptune .5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati"
- the section called "[Neptune .6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive"
- the section called "[Neptune .7] I cluster Neptune DB devono avere l'autenti cazione del database IAM abilitata"
- the section called "[Neptune .8] I cluster Neptune DB devono essere configura ti per copiare i tag nelle istantanee"
- the section called "[RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi"

Visualizzazione dei controlli consolidati e risultati di controllo consolidati disponibili in AWS GovCloud (US)	La visualizzazione dei controlli consolidati e i risultati del controllo consolidato sono ora disponibili in. AWS GovCloud (US) Region La pagina Controlli della console CSPM di Security Hub mostra tutti i controlli tra gli standard. Ogni controllo ha lo stesso ID di controllo per tutti gli standard. Quando attivi i risultati del controllo consolidato, ricevi un solo risultato per controllo di sicurezza anche quando un controllo si applica a più standard abilitati.	6 settembre 2023
Visualizzazione dei controlli consolidati e risultati del controllo consolidato disponibili nelle regioni della Cina	La visualizzazione dei controlli consolidati e i risultati del controllo consolidato sono ora disponibili nelle regioni della Cina. La pagina Controlli della console CSPM di Security Hub mostra tutti i controlli tra gli standard. Ogni controllo ha lo stesso ID di controllo per tutti gli standard. Quando attivi i risultati del controllo consolidato, ricevi un solo risultato per controllo di sicurezza anche quando un controllo si applica a più standard abilitati.	28 agosto 2023

Security Hub CSPM disponibile nella regione di Israele (Tel Aviv)	Security Hub CSPM è ora disponibile in Israele (Tel Aviv). Tutte le funzionalità CSPM di Security Hub sono ora disponibili in questa regione, ad eccezione di alcuni controlli di sicurezza. Per ulteriori informazioni, vedere Disponibilità dei controlli per regione.	8 agosto 2023

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub: • [Athena.1] I gruppi di lavoro Athena devono essere crittografati quando sono inattivi • the section called "[DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi" • the section called "[DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato" • the section called "[Neptune .1] I cluster Neptune DB devono essere crittografati quando sono inattivi" • the section called "[Neptune .2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch" • the section called "[Neptune .3] Le istantanee del cluster Neptune DB non devono essere pubbliche" • the section called "[Neptune .4] I cluster Neptune DB dovrebbero avere la	28 luglio 2023

	protezione da eliminazione abilitata" • the section called "[Neptune .5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati" • the section called "[Neptune .6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive" • the section called "[Neptune .7] I cluster Neptune DB devono avere l'autenti cazione del database IAM abilitata" • the section called "[Neptune .8] I cluster Neptune DB devono essere configura ti per copiare i tag nelle istantanee" • the section called "[RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi"	
Nuovi operatori per i criteri delle regole di automazione	Ora puoi utilizzare gli operatori di confronto CONTAINS e NOT_CONTAINS per la mappa delle regole di automazione e i criteri delle stringhe.	25 luglio 2023

Regole di automazione	Security Hub CSPM ora offre regole di automazione che aggiornano automaticamente i risultati in base a criteri specificati dall'utente.	13 giugno 2023
Nuova integrazione con terze parti	Snykè una nuova integrazione di terze parti che invia i risultati a Security Hub CSPM.	12 giugno 2023

Controlli di sicurezza esistenti aggiunti a Service-Managed Standard: AWS Control Tower	I seguenti controlli CSPM di Security Hub esistenti sono stati aggiunti a Service-Managed Standard:. AWS Control Tower • the section called "[Account.1] Le informazioni di contatto per la sicurezza devono essere fornite per un Account AWS" • the section called "[APIGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione" • the section called "[APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages" • the section called "[CodeBuild.3] I log CodeBuild S3 devono essere crittografati" • the section called "[EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete" • the section called "[ELB.1] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS" • the section called "[Redshift.10] I cluster Redshift	12 giugno 2023

devono essere crittografati a riposo"

- the section called "[SageMaker.2] le istanze di SageMaker notebook devono essere avviate in un VPC personalizzato"
- the section called "[SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook"
- the section called "[WAF.10] AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole"

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub: • the section called "[ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit" • the section called "[AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata" • the section called "[CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine" • the section called "[Elastic Beanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch" • the section called "[S3.17] I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys" • the section called "[StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata"	6 giugno 2023

Security Hub CSPM disponibile in Asia Pacifico (Melbourne)	Security Hub CSPM è ora disponibile in Asia Pacifico (Melbourne). Tutte le funzionalità CSPM di Security Hub sono ora disponibili in questa regione, ad eccezione di alcuni controlli di sicurezza. Per ulteriori informazioni, vedere Disponibilità dei controlli per regione.	25 maggio 2023
Ricerca della cronologia	Security Hub CSPM può ora tenere traccia della cronologia di un ritrovamento negli ultimi 90 giorni.	4 maggio 2023
Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub: • the section called "[EKS.1] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico" • the section called "[ELB.16] Application Load Balancers deve essere associato a un AWS WAF ACL Web" • the section called "[Redshift.10] I cluster Redshift devono essere crittografati a riposo" • the section called "[S3.15] I bucket generici S3 devono avere Object Lock abilitato"	29 marzo 2023

Supporto esteso per risultati di controllo consolidati	L'Automated Security Response nella versione AWS 2.0.0 ora supporta i risultati di controllo consolidati.	24 marzo 2023
Security Hub CSPM disponibile in nuove versioni Regioni AWS	Security Hub CSPM è ora disponibile in Asia Pacifico (Hyderabad), Europa (Spagna) ed Europa (Zurigo). Esistono dei limiti ai controlli disponibili in queste regioni.	21 marzo 2023
Aggiornamento della politica gestita	Security Hub CSPM ha aggiornato un'autorizzazione esistente nella politica `AWSSecurityHubServiceRolePolicy` gestita.	17 marzo 2023

Nuovi controlli di sicurezza per lo standard NIST 800-53	Security Hub CSPM ha aggiunto i seguenti controlli di sicurezza, applicabili allo standard NIST 800-53: • the section called "[Account.2] Account AWS dovrebbe far parte di un AWS Organizations organizzazione" • the section called "[CloudWatch.15] gli CloudWatch allarmi dovrebbero avere azioni specificate configurate" • the section called "[CloudWatch.16] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato" • the section called "[CloudWatch.17] le azioni CloudWatch di allarme devono essere attivate" • the section called "[DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup" • the section called "[EC2.28] I volumi EBS devono essere coperti da un piano di backup"	3 marzo 2023

	• EC2.29 — Le istanze EC2 devono essere avviate in un VPC (ritirato) • the section called "[RDS.26] Le istanze DB RDS devono essere protette da un piano di backup" • the section called "S3.14[] I bucket S3 per uso generico devono avere il controllo delle versioni abilitato" • the section called "[WAF.11] AWS WAF la registrazione ACL web deve essere abilitata"	
Istituto nazionale di standard e tecnologia (NIST) 800-53 Rev. 5	Security Hub CSPM ora supporta lo standard NIST 800-53 Rev. 5 con più di 200 controlli di sicurezza applicabili.	28 febbraio 2023
I controlli consolidati visualizzano e controllano i risultati	Con il rilascio della visualizzazione dei controlli consolidati, la pagina Controlli della console Security Hub CSPM mostra tutti i controlli tra gli standard. Ogni controllo ha lo stesso ID di controllo per tutti gli standard. Quando attivi i risultati del controllo consolidato, ricevi un solo risultato per controllo di sicurezza anche quando un controllo si applica a più standard abilitati.	23 febbraio 2023

Nuovi controlli di sicurezza	Sono disponibili i seguenti nuovi controlli CSPM di Security Hub. Alcuni controlli hanno limitazioni regionali. • the section called "I cluster [ElastiCache.1] ElastiCache (Redis OSS) devono avere i backup automatici abilitati" • the section called "[ElastiCache.2] i ElastiCache cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati" • the section called "[ElastiCache.3] i gruppi di ElastiCache replica devono avere il failover automatico abilitato" • the section called "[ElastiCache.4] i gruppi di ElastiCache replica devono essere crittografati quando sono inattivi" • the section called "[ElastiCache.5] i gruppi di ElastiCache replica devono essere crittografati in transito" • the section called "[ElastiCache.6] ElastiCache (Redis OSS) i gruppi di replica delle versioni precedenti devono avere Redis OSS AUTH abilitato"	16 febbraio 2023

	• the section called "[ElastiCache.7] i ElastiCache cluster non devono utilizzare il gruppo di sottoreti predefinito"	
Nuovi campi ASFF	Security Hub CSPM è stato aggiunto ProductFields.ArchivalReasons:0/Description ProductFields.ArchivalReasons:0/ReasonCode al AWS Security Finding Format (ASFF).	8 febbraio 2023
Nuovi campi ASFF	Security Hub CSPM è stato aggiunto Compliance.AssociatedStandards Compliance.SecurityControlId al AWS Security Finding Format (ASFF).	31 gennaio 2023
I dettagli sulla vulnerabilità sono ora disponibili	Ora puoi visualizzare i dettagli delle vulnerabilità nella console CSPM di Security Hub per i risultati che Amazon Inspector invia a Security Hub CSPM.	14 gennaio 2023
Security Hub CSPM è disponibile in Medio Oriente (Emirati Arabi Uniti)	Security Hub CSPM è ora disponibile in Medio Oriente (Emirati Arabi Uniti). Alcuni controlli hanno limiti regionali.	12 gennaio 2023
È stata aggiunta l'integrazione di terze parti con MetricStream	Security Hub CSPM ora supporta l'integrazione di terze parti MetricStream in tutte le regioni tranne Cina e. AWS GovCloud (US)	11 gennaio 2023

Aumento del limite degli account organizzativi	Security Hub CSPM ora supporta fino a 11.000 account membro per ogni account amministratore CSPM di Security Hub per regione.	27 dicembre 2022
ElasticBeanstalk.3 arrotolato indietro	Security Hub CSPM ha ripristinato il controllo [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log CloudWatch dallo standard FSBP in tutte le regioni.	21 dicembre 2022
Security Hub CSPM aggiunge nuovi controlli di sicurezza	I nuovi controlli CSPM di Security Hub sono disponibili per i clienti che hanno abilitato lo standard FSBP. Alcuni controlli hanno limitazioni regionali.	15 dicembre 2022
Linee guida sulle funzionalità imminenti	Security Hub CSPM prevede di rilasciare due nuove funzionalità: visualizzazione dei controlli consolidati e risultati del controllo consolidato. Queste funzionalità imminenti potrebbero influire sui flussi di lavoro esistenti che si basano sul controllo della ricerca di campi e valori.	9 dicembre 2022
L'integrazione con Amazon Security Lake è ora disponibile	Security Lake ora si integra con Security Hub CSPM ricevendo i risultati CSPM di Security Hub.	29 novembre 2022

Support per Service-Managed Standard: AWS Control Tower	Security Hub CSPM supporta un nuovo standard di sicurezza chiamato Service-Managed Standard:. AWS Control Tower AWS Control Tower gestisce questo standard.	28 novembre 2022
CIS AWS Foundations Benchmark v1.4.0 ora disponibile nelle regioni della Cina	Security Hub CSPM ora supporta CIS AWS Foundations Benchmark v1.4.0 nelle regioni della Cina.	18 novembre 2022
L'integrazione con Jira Service Management Cloud è ora disponibile	Jira Service Management Cloud ora riceve i risultati CSPM di Security Hub in tutte le regioni disponibili, ad eccezione delle regioni della Cina.	17 novembre 2022
AWS IoT Device Defender integrazione ora disponibile	AWS IoT Device Defender ora invia i risultati al Security Hub CSPM in tutte le regioni disponibili.	17 novembre 2022
Support per CIS AWS Foundations Benchmark v1.4.0	Security Hub CSPM ora fornisce controlli di sicurezza che supportano CIS Foundations Benchmark AWS v1.4.0. Questo standard è disponibile in tutte le regioni disponibili, ad eccezione delle regioni della Cina.	09 novembre 2022

Supporto per gli annunci CSPM di Security Hub in AWS GovCloud (US)	Ora puoi iscriverti agli annunci CSPM di Security Hub con Amazon AWS GovCloud Simple Notification Service (Amazon SNS) US-East in () US-West e (AWS GovCloud) per ricevere notifiche su Security Hub CSPM.	3 ottobre 2022
AWS Security Hub CSPM aggiunge un nuovo controllo di sicurezza	Il nuovo controllo CSPM Security Hub AutoScaling.9è disponibile per i clienti che hanno abilitato lo standard FSBP. I controlli possono avere limitazioni regionali.	1 settembre 2022
Iscriviti agli annunci CSPM di Security Hub	Ora puoi iscriverti agli annunci CSPM di Security Hub con Amazon Simple Notification Service (Amazon SNS) per ricevere notifiche su Security Hub CSPM.	29 agosto 2022
Espansione regionale per l'aggregazione tra regioni	Cross-Region l'aggregazione è ora disponibile per i risultati , la ricerca di aggiornamenti e approfondimenti in tutto il mondo. AWS GovCloud (US)	2 agosto 2022
Nuove integrazioni di prodotti di terze parti	Fortinet - FortiCNP è un'integrazione di terze parti che riceve i risultati CSPM di Security Hub e JFrog è un'integrazione di terze parti che invia i risultati a Security Hub CSPM.	26 luglio 2022

EC2.27 è in pensione	Security Hub CSPM è stato ritirato EC2.27 : le istanze EC2 in esecuzione non devono utilizzare coppie di chiavi, un controllo precedente dello standard AWS Found ational Security Best Practices (FSBP).	20 luglio 2022
Lambda.2 non supporta più python3.6	Security Hub CSPM non supporta più python3.6 come parametro per Lambda.2 : le funzioni Lambda devono utilizzare runtime supportat i, un controllo nello standard Foundational Security Best Practices (FSBP). AWS	19 luglio 2022
AWS Security Hub CSPM aggiunge nuovi controlli di sicurezza	I nuovi controlli CSPM di Security Hub sono disponibili per i clienti che hanno abilitato lo standard FSBP. Alcuni controlli hanno limitazioni regionali.	22 giugno 2022
AWS Security Hub CSPM supporta una nuova regione	Security Hub CSPM è ora disponibile in Asia Pacifico (Giacarta). Alcuni controlli non sono disponibili in questa regione.	7 luglio 2022
Migliore integrazione tra AWS Security Hub CSPM e AWS Config	Gli utenti di Security Hub CSPM possono vedere i risultati delle valutazioni delle AWS Config regole come risultati in Security Hub CSPM.	6 giugno 2022

Aggiunta la possibilità di disattivare gli standard con attivazione automatica	Per gli utenti che hanno effettuato l'integrazione con AWS Organizations, questa funzionalità consente di accedere all'account amministratore CSPM di Security Hub e disattivare gli account dei nuovi membri dagli standard di attivazione automatica.	25 aprile 2022
Aggregazione estesa tra regioni	Aggiunta l'aggregazione tra regioni per controllare gli stati e i punteggi di sicurezza.	20 aprile 2022
CompanyName e ora ProductName sono attributi di primo livello	Sono stati aggiunti nuovi attributi di primo livello per l'impostazione dei nomi di società e prodotti associati alle integrazioni personalizzate	1 aprile 2022
Aggiunti nuovi controlli allo standard AWS Foundational Security Best Practices	Sono stati aggiunti 5 nuovi controlli allo standard AWS Foundational Security Best Practices.	31 marzo 2022
Aggiunti nuovi oggetti di dettaglio delle risorse ad ASFF	È stato aggiunto un tipo di `AwsRdsDbSecurityGroup` risorsa ad ASFF.	25 marzo 2022
Sono stati aggiunti dettagli aggiuntivi sulle risorse in ASFF	Sono stati aggiunti ulteriori dettagli a `AwsAutoScalingScalingGroup` `AwsElbLoadBalancer` ,`AwsRedshiftCluster` , e`AwsCodeBuildProject` .	25 marzo 2022

Sono stati aggiunti nuovi controlli allo standard AWS Foundational Security Best Practices	Aggiunti 15 nuovi controlli allo standard AWS Foundational Security Best Practices.	16 marzo 2022
Sono stati aggiunti nuovi controlli allo standard AWS Foundational Security Best Practices e al Payment Card Industry Data Security Standard (PCI DSS)	Sono stati aggiunti nuovi controlli per Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing e AWS allo standard Foundational CloudFront Security Best Practices. Sono stati inoltre aggiunti due nuovi controlli per OpenSearch Service al PCI DSS.	15 febbraio 2022
Aggiunto un nuovo campo ad ASFF	Nuovo campo aggiunto: Sample.	26 gennaio 2022
Aggiunta integrazione con AWS Health	AWS Health utilizza la messaggistica di eventi da servizio a servizio per inviare i risultati al Security Hub CSPM.	19 gennaio 2022
Aggiunta integrazione con AWS Trusted Advisor	Trusted Advisor invia i risultati dei controlli a Security Hub CSPM come risultati CSPM di Security Hub. Security Hub CSPM invia i risultati dei suoi controlli sulle migliori pratiche di sicurezza AWS fondament ali a. Trusted Advisor	18 gennaio 2022

Oggetti aggiornati con i dettagli delle risorse in ASFF	Aggiunti `MixedInstancesPolicy` e `AvailabilityZones` a `AwsAutoScalingAutoScalingGroup`. Aggiunto `MetadataOptions` a `AwsAutoScalingLaunchConfiguration`. Aggiunto `BucketVersioningConfiguration` a `AwsS3Bucket`.	20 dicembre 2021
Output aggiornato per la documentazione ASFF	Le descrizioni degli attributi ASFF erano precedentemente contenute in un unico argomento. Ogni oggetto di primo livello e ogni oggetto relativo ai dettagli delle risorse ora si trova in un argomento a sé stante. L'argomento sulla sintassi ASFF contiene collegamenti a tali argomenti.	20 dicembre 2021
Sono stati aggiunti nuovi oggetti di dettaglio delle risorse ad ASFF per AWS Network Firewall	Per AWS Network Firewall, sono stati aggiunti i seguenti oggetti di dettaglio delle risorse: `AwsNetworkFirewallFirewall` `AwsNetworkFireFirewallPolicy`, e `AwsNetworkFirewallRuleGroup`.	20 dicembre 2021

È stato aggiunto il supporto per la nuova versione di Amazon Inspector	Security Hub CSPM è integrato con la nuova versione di Amazon Inspector e con Amazon Inspector Classic. Amazon Inspector invia i risultati al Security Hub CSPM.	29 novembre 2021
È stata modificata la gravità di EC2.19	La gravità di EC2.19 (i gruppi di sicurezza non dovrebbero consentire l'accesso illimitato alle porte ad alto rischio) è stata modificata da Alta a Critica.	17 novembre 2021
Nuova integrazione con Sonrai Dig	Security Hub CSPM ora offre un'integrazione con. Sonrai Dig Sonrai Digmonitora gli ambienti cloud per identificare i rischi per la sicurezza. Sonrai Diginvia i risultati al Security Hub CSPM.	12 novembre 2021
Controllo aggiornato per CIS 2.1 e controlli CloudTrail.1	Oltre a verificare che sia presente almeno un CloudTrail percorso multiregionale, ora CIS 2.1 CloudTrail.1 controlla anche che `ExcludeManagementEventSources` il parametro sia vuoto in almeno uno dei CloudTrail percorsi multiregione.	9 novembre 2021
Aggiunto il supporto per gli endpoint VPC	Security Hub CSPM è ora integrato AWS PrivateLink e supporta gli endpoint VPC.	03 novembre 2021

Controlli aggiunti allo standard AWS Foundational Security Best Practices	Aggiunti nuovi controlli per Elastic Load Balancing (ELB.2 and ELB.8) e AWS Systems Manager (SSM.4).	2 novembre 2021
Porte aggiunte alla verifica del EC2.19 controllo	EC2.19 ora verifica anche che i gruppi di sicurezza non consentano l'accesso illimitato in ingresso alle seguenti porte: 3000 (framework di sviluppo web Go e Ruby), 5000 (framework di sviluppo web Python), 8088 (porta HTTP legacy) e 8888 (porta HTTP alternativa) Node.js	27 ottobre 2021
È stata aggiunta l'integrazione con Cloud SIEM Logz.io	Logz.io è un fornitore di Cloud SIEM che fornisce una correlazione avanzata di dati di log ed eventi per aiutare i team di sicurezza a rilevare, analizzare e rispondere alle minacce alla sicurezza in tempo reale. Logz.io riceve i risultati dal Security Hub CSPM.	25 ottobre 2021

È stato aggiunto il supporto per l'aggregazione dei risultati tra regioni	Cross-Region l'aggregazione consente di visualizzare tutti i risultati senza dover cambiare regione. Gli account amministratore scelgono una regione di aggregazione e le regioni collegate. I risultati relativi all'account amministratore e ai relativi account membro vengono aggregati dalle regioni collegate alla regione di aggregazione.	20 ottobre 2021
Oggetti aggiornati con i dettagli delle risorse in ASFF	Sono stati aggiunti i dettagli del certificato del visualizzatore a. `AwsCloudFrontDistribution` Sono stati aggiunti dettagli aggiuntivi a`AwsCodeBuildProject` . Sono stati aggiunti gli attributi del load balancer a. `AwsElbV2LoadBalancer` È stato aggiunto l'identificatore dell'account del proprietario del bucket S3 a. `AwsS3Bucket`	8 ottobre 2021

Aggiunti nuovi oggetti di dettaglio delle risorse ad ASFF	Sono stati aggiunti i seguenti nuovi oggetti di dettaglio delle risorse ad ASFF:`AwsEc2VpcEndpointService` ,,`AwsEcrRepository` ,`AwsEksCluster` ,,`AwsOpenSearchServiceDomain` , `AwsWafRateBasedRule` `AwsWafRegionalRateBasedRule` `AwsXrayEncryptionConfig`	8 ottobre 2021
Il runtime obsoleto è stato rimosso dal controllo Lambda.2	Nello standard AWS Foundational Security Best Practices, il `dotnetcore2.1` runtime rimosso da [Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati.	6 ottobre 2021
Nuovo nome per l'integrazione con Check Point	L'integrazione con Check Point Dome9 Arc è ora Check Point CloudGuard Posture Management. L'ARN di integrazione non è cambiato.	1° ottobre 2021
Rimossa l'integrazione con Alcide	L'integrazione con Alcide KAudit è stata interrotta.	30 settembre 2021
È stata modificata la gravità di EC2.19	La severità di [EC2.19] I gruppi di sicurezza non dovrebbero consentire l'accesso illimitato alle porte ad alto rischio è stata modificata da Media a Alta.	30 settembre 2021

L'integrazione con AWS Organizations è ora supportata nelle regioni della Cina	L'integrazione CSPM di Security Hub con Organizations è ora supportata in Cina (Pechino) e Cina (Ningxia).	20 settembre 2021
Nuova AWS Config regola per i controlli e S3.1 PCI.S3.6	Entrambi S3.1 e PCI.S3.6 verifica che l'impostazione Amazon S3 Block Public Access sia abilitata. La AWS Config regola per questi controlli viene modificata da `s3-account-level-public-access-blocks` a `s3-account-level-public-access-blocks-periodic` .	14 settembre 2021
I runtime obsoleti sono stati rimossi dal controllo Lambda.2	Nello standard AWS Foundational Security Best Practices, i `ruby2.5` runtime `nodejs10.x` e i runtime rimossi da [] Lambda.2 Lambda devono utilizzare i runtime supportati.	13 settembre 2021
Modificata la severità del controllo CIS 2.2	Nello standard CIS AWS Foundations Benchmark, la severità per 2.2. — La verifica che la convalida dei file di CloudTrail registro sia abilitata viene modificata da Bassa a Media.	13 settembre 2021

Aggiornato ECS.1 e Lambda.2 SSM.1 conforme allo standard AWS Foundational Security Best Practices	Nello standard AWS Foundational Security Best Practices, ECS.1 ora ha un `SkipInactiveTaskDefinitions` parametro impostato su. `true` Ciò garantisce che il controllo controlli solo le definizioni delle attività attive. Per Lambda.2, ha aggiunto Python 3.9 all'elenco dei runtime. SSM.1 ora controlla sia le istanze interrotte che quelle in esecuzione.	7 settembre 2021
PCI.Lambda.2 il controllo ora esclude le risorse Lambda @Edge	Nello standard Payment Card Industry Data Security Standard (PCI DSS), il PCI.Lambda.2 controllo ora esclude le risorse Lambda @Edge.	7 settembre 2021
È stata aggiunta l'integrazione con HackerOne Vulnerability Intelligence	Security Hub CSPM ora offre un'integrazione con. HackerOne Vulnerability Intelligence L'integrazione invia i risultati a Security Hub CSPM.	7 settembre 2021

Oggetti aggiornati con i dettagli delle risorse in ASFF	PerAwsKmsKey , aggiuntoKeyRotationStatus . PerAwsS3Bucket , ha aggiunto AccessControlList BucketLoggingConfiguration ,BucketNotificationConfiguration , eBucketWebsiteConfiguration .	2 settembre 2021
Sono stati aggiunti nuovi oggetti di dettaglio delle risorse ad ASFF	Sono stati aggiunti i seguenti nuovi oggetti di dettaglio delle risorse ad ASFF: AwsAutoScalingLaunchConfiguration AwsEc2VpnConnection , e. AwsEcrContainerImage	2 settembre 2021
Sono stati aggiunti dettagli all'Vulnerabilities oggetto in ASFF	InCvss, aggiunto Adjustments e. Source InVulnerablePackages , ha aggiunto il percorso del file e il gestore dei pacchetti.	2 settembre 2021
Systems Manager Explorer e OpsCenter integrazione ora supportati nelle regioni della Cina	Il Security Hub CSPM si integra con SSM Explorer ed OpsCenter è ora supportato in Cina (Pechino) e Cina (Ningxia).	31 agosto 2021

Ritiro del controllo Lambda.4	Security Hub CSPM sta ritirando il controllo [] Le funzioni Lambda.4 Lambda dovrebbero avere una coda di lettere non scritte configura ta. Quando un controllo viene ritirato, non viene più visualizz ato sulla console e Security Hub CSPM non esegue controlli su di esso.	31 agosto 2021
Ritiro del controllo PCI.EC2.3	Security Hub CSPM sta ritirando il controllo [PCI.EC2. 3] I gruppi di sicurezza EC2 non utilizzati devono essere rimossi. Quando un controllo viene ritirato, non viene più visualizzato sulla console e Security Hub CSPM non esegue controlli su di esso.	27 agosto 2021
Cambia il modo in cui Security Hub CSPM invia i risultati alle azioni personalizzate	Quando invii i risultati a un'azione personalizzata, Security Hub CSPM ora invia ogni risultato in un evento separato Security Hub Findings - Custom Action.	20 agosto 2021

Aggiunto un nuovo codice motivo dello stato di conformità per i runtime Lambda personalizzati	È stato aggiunto un nuovo codice motivo dello stato di conformità. `LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE` Questo codice motivo indica che Security Hub CSPM non è stato in grado di eseguire un controllo rispetto a un runtime Lambda personalizzato.	20 agosto 2021
AWS Firewall Manager integrazione ora supportata nelle regioni della Cina	L'integrazione CSPM di Security Hub con Firewall Manager è ora supportata in Cina (Pechino) e Cina (Ningxia).	19 agosto 2021
Nuove integrazioni con e Caveonix CloudForcepoint Cloud Security Gateway	Security Hub CSPM ora offre integrazioni con e. Caveonix Cloud Forcepoint Cloud Security Gateway Entrambe le integrazioni inviano i risultati al Security Hub CSPM.	10 agosto 2021

Sono stati aggiunti nuovi `CompanyName` attributi e `ProductName` ad ASFF `Region`	Aggiunti `CompanyName` `Region` campi e al livello superiore dell'ASFF. `ProductName` Questi campi vengono compilati automaticamente e, ad eccezione delle integrazioni di prodotti personalizzati, non possono essere aggiornati utilizzando o. `BatchImportFindings` `BatchUpdateFindings` Sulla console, i filtri di ricerca utilizzano questi nuovi campi. Nell'API, i `ProductName` filtri `CompanyName` and utilizzano gli attributi sottostanti`ProductFields` .	23 luglio 2021
Oggetti di dettaglio delle risorse aggiunti e aggiornati in ASFF	Sono stati aggiunti un nuovo tipo di `AwsRdsEventSubscription` risorsa e nuovi dettagli sulla risorsa. Sono stati aggiunti dettagli sulla risorsa per il tipo di `AwsEcsService` risorsa. Sono stati aggiunti attributi all'oggetto dei dettagli della `AwsElasticsearchDomain` risorsa.	23 luglio 2021

Sono stati aggiunti controlli allo standard AWS Foundational Security Best Practices	Sono stati aggiunti nuovi controlli per Amazon API Gateway (APIGateway.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon Service (ES.5 tramite ES.8), OpenSearch Amazon RDS (tramiteRDS.16) RDS.23, Amazon Redshift () e Amazon SQS (Redshift.4). SQS.1	20 luglio 2021
È stata spostata un'autorizzazione all'interno della politica di gestione dei ruoli collegati al servizio	L'`config:PutEvaluations` autorizzazione è stata spostata all'interno della politica gestita`AWSSecurityHubServiceRolePolicy` , in modo che venga applicata a tutte le risorse.	14 luglio 2021
Sono stati aggiunti controlli allo standard AWS Foundational Security Best Practices	Sono stati aggiunti nuovi controlli per Amazon API Gateway CloudFront (APIGateway.4), Amazon (CloudFront.5 and CloudFront.6), Amazon EC2 (EC2.17 and EC2.18), Amazon ECS ()ECS.1, Amazon OpenSearch Service (ES.4), AWS Identity and Access Management ()IAM.21, Amazon RDS (RDS.15) e Amazon S3 (). S3.8	08 luglio 2021

Sono stati aggiunti nuovi codici motivazionali relativi allo stato di conformità per i risultati del controllo	`INTERNAL_SERVICE_ERROR` indica che si è verificato un errore sconosciuto. `SNS_TOPIC_CROSS_ACCOUNT` indica che l'argomento SNS è di proprietà di un account diverso. `SNS_TOPIC_INVALID` indica che l'argomento SNS associato non è valido.	6 luglio 2021
Aggiunta l'integrazione con Amazon Q Developer nelle applicazioni di chat	È stata aggiunta l'integrazione con Amazon Q Developer nelle applicazioni di chat. Security Hub CSPM invia i risultati ad Amazon Q Developer nelle applicazioni di chat.	30 giugno 2021
È stata aggiunta una nuova autorizzazione alla politica di gestione dei ruoli collegati al servizio	È stata aggiunta una nuova autorizzazione alla policy gestita `AWSSecurityHubServiceRolePolicy` per consentire al ruolo collegato al servizio di fornire risultati di valutazione a. AWS Config	29 giugno 2021

Oggetti di dettaglio delle risorse nuovi e aggiornati nell'ASFF	Sono stati aggiunti nuovi oggetti di dettaglio delle risorse per i cluster ECS e le definizioni delle attività ECS. È stato aggiornato l'oggetto dell'istanza EC2 per elencare le interfacce di rete associate . È stato aggiunto l'ID del certificato client per le fasi API Gateway V2. È stata aggiunta la configurazione del ciclo di vita per i bucket S3.	24 giugno 2021
Aggiornato il calcolo degli stati di controllo aggregati e dei punteggi di sicurezza standard	Security Hub CSPM ora calcola lo stato di controllo complessivo e il punteggio di sicurezza standard ogni 24 ore. Per gli account amministratore, il punteggio ora indica se ogni controllo è abilitato o disabilitato per ogni account.	23 giugno 2021
Informazioni aggiornate sulla gestione CSPM di Security Hub degli account sospesi	Sono state aggiunte informazioni su come Security Hub CSPM gestisce gli account sospesi. AWS	23 giugno 2021

Sono state aggiunte schede per visualizzare i controlli abilitati e disabilitati per il singolo account amministratore	Per l'account amministratore, le schede principali della pagina dei dettagli standard contengono informazioni aggregate su tutti gli account. Le nuove schede Abilitato per questo account e Disabilitato per questo account elencano gli account abilitati o disabilitati per il singolo account amministratore.	23 giugno 2021
Aggiunto `java8.al2` ai parametri per `Lambda.2`	Nello standard AWS Foundational Security Best Practices, aggiunto `java8.al2` ai runtime supportati per il `Lambda.2` controllo.	08 giugno 2021
Nuove integrazioni con NETSCOUT Cyber MicroFocus ArcSight Investigator	Aggiunte integrazioni con NETSCOUT Cyber Investigator. MicroFocus ArcSight MicroFocus ArcSight riceve i risultati dal Security Hub CSPM. NETSCOUT Cyber Investigator invia i risultati al Security Hub CSPM.	7 giugno 2021
Sono stati aggiunti dettagli per `AWSSecurityHubServiceRolePolicy`	È stata aggiornata la sezione delle politiche gestite per aggiungere dettagli per la politica gestita esistente `AWSSecurityHubServiceRolePolicy`, utilizzata dal ruolo collegato al servizio Security Hub CSPM.	4 giugno 2021

Nuova integrazione con Jira Service Management	Il AWS Service Management Connector per Jira invia i risultati a Jira e li usa per creare problemi con Jira. Quando i problemi di Jira vengono aggiornati, vengono aggiornati anche i risultati corrispondenti in Security Hub CSPM.	26 maggio 2021
È stato aggiornato l'elenco dei controlli supportati per la regione Asia Pacifico (Osaka)	Sono stati aggiornati lo standard CIS AWS Foundations e il Payment Card Industry Data Security Standard (PCI DSS) per indicare i controlli che non sono supportati in Asia Pacifico (Osaka).	21 maggio 2021
Nuova integrazione con Sysdig Secure per il cloud	Aggiunta un'integrazione con Sysdig Secure per il cloud. L'integrazione invia i risultati a Security Hub CSPM.	14 maggio 2021

Controlli aggiunti allo standard AWS Foundational Security Best Practices	Aggiunti nuovi controlli per Amazon API Gateway (APIGateway.2 and APIGateway.3), AWS CloudTrail (CloudTrail.4 and CloudTrail.5), Amazon EC2 (EC2.15 and EC2.16), AWS Elastic Beanstalk (Elastic Beanstalk.1 and ElasticBe anstalk.2), AWS Lambda (Lambda.4), Amazon RDS (RDS.12— RDS.14), Amazon Redshift (Redshift.7), (and) SecretsManager.3 e AWS Secrets Manager (SecretsMa nager.4). AWS WAF WAF.1	10 maggio 2021
Aggiornamenti GuardDuty e controlli Amazon RDS	È stata modificata la gravità `GuardDuty.1` `PCI.Guard Duty.1` da Media a Alta. È stato aggiunto un `databaseE ngines` parametro a`RDS.8`.	04 maggio 2021
Sono stati aggiunti nuovi dettagli sulle risorse all'ASFF	Nel`Resources.Details` , sono stati aggiunti nuovi oggetti di dettaglio delle risorse per gli ACL di rete Amazon EC2, le sottoreti Amazon EC2 e gli ambienti. AWS Elastic Beanstalk	3 maggio 2021
Aggiunti campi della console per fornire valori di filtro per EventBridge le regole di Amazon	I nuovi modelli di filtro predefini ti per le EventBridge regole CSPM di Security Hub forniscono campi della console che è possibile utilizzare per specificare i valori del filtro.	30 aprile 2021

È stata aggiunta l'integrazione con Explorer e AWS Systems Manager OpsCenter	Security Hub CSPM ora supporta l'integrazione con Systems Manager Explorer e. OpsCenter L'integrazione riceve i risultati da Security Hub CSPM e li aggiorna in Security Hub CSPM.	26 Aprile 2021
Nuovo tipo di integrazione dei prodotti	Un nuovo tipo di integrazione indica che `UPDATE_FINDINGS_IN_SECURITY_HUB` l'integrazione di un prodotto aggiorna i risultati ricevuti dal Security Hub CSPM.	22 aprile 2021
Il termine "account principale" è stato modificato in "account amministratore"	Il termine "account principale" viene modificato in "account amministratore". Il termine viene modificato anche nella console CSPM e nell'API di Security Hub.	22 aprile 2021
Aggiornato APIGateway.1 per sostituire HTTP con Websocket	Sono stati aggiornati il titolo, la descrizione e la correzione per. APIGateway.1 Il controllo ora verifica la registrazione dell'esecuzione dell'API Websocket anziché la registrazione dell'esecuzione dell'API HTTP.	09 aprile 2021
GuardDuty L'integrazione con Amazon è ora supportata a Pechino e Ningxia	L'integrazione con Security Hub CSPM GuardDuty è ora supportata nelle regioni Cina (Pechino) e Cina (Ningxia).	5 aprile 2021

Aggiunto `nodejs14.x` ai runtime supportati per il controllo Lambda.2	Il Lambda.2 controllo dello standard Foundational Security Best Practices ora supporta il `nodejs14.x` runtime.	30 marzo 2021
Lancio del Security Hub CSPM in Asia Pacifico (Osaka)	Security Hub CSPM è ora disponibile nella regione Asia Pacifico (Osaka).	29 marzo 2021
Sono stati aggiunti i campi di ricerca del provider alla ricerca dei dettagli	Nel pannello dei dettagli dei risultati, la nuova sezione Finding Provider Fields contiene i valori del provider di ricerca relativi a fiducia, criticità, risultati correlati, gravità e tipi.	24 marzo 2021
Aggiunta l'opzione per ricevere dati sensibili da Amazon Macie	L'integrazione con Macie può ora essere configurata per inviare risultati sensibili a Security Hub CSPM.	23 marzo 2021
Passaggio alla gestione degli account AWS Organizations	Per i clienti che dispongon o di un account amministr atore esistente con account membro, sono state aggiunte nuove informazioni su come passare dalla gestione degli account su invito alla gestione degli account tramite Organizations.	22 marzo 2021

Nuovi oggetti in ASFF per informazioni sulla configurazione del blocco di accesso pubblico di Amazon S3	Nel `Resources` , un nuovo tipo di `AwsS3AccountPublicAccessBlock` risorsa e un nuovo oggetto di dettaglio forniscono informazioni sulla configurazione del blocco di accesso pubblico di Amazon S3 per gli account. Nell'oggetto `AwsS3Bucket` Resource Details, l'`PublicAccessBlockConfiguration` oggetto fornisce la configurazione Public Access Block per il bucket S3.	18 marzo 2021
Nuovo oggetto in ASFF per consentire ai provider di ricerca di aggiornare campi specifici	Il nuovo `FindingProviderFields` oggetto in ASFF viene utilizzato per `BatchImportFindings` fornire valori per`Confidence` ,, `Criticality` `RelatedFindings` `Severity`, e. `Types` I campi originali devono essere aggiornati solo utilizzando`BatchUpdateFindings` .	18 marzo 2021
Nuovo `DataClassification` oggetto per le risorse in ASFF	Il nuovo `Resources.DataClassification` oggetto in ASFF viene utilizzato per fornire informazioni sui dati sensibili rilevati sulla risorsa.	18 marzo 2021

CONFIG_RETURNS_NOT_APPLICABLE Valore aggiunto ai codici di stato di conformità disponibili	Per lo stato di NOT_AVAILABLE conformità, è stato rimosso il codice motivo RESOURCE_NO_LONGER_EXISTS e aggiunto il codice motivoCONFIG_RETURNS_NOT_APPLICABLE .	16 marzo 2021
Nuova politica gestita per l'integrazione con AWS Organizations	Una nuova policy gestita fornisce AWSSecurityHubOrganizationsAccess le autorizzazioni Organizations necessarie all'account di gestione dell'organizzazione e all'account amministratore CSPM di Security Hub delegato.	15 marzo 2021
Le informazioni sulla politica gestita e sui ruoli collegati ai servizi sono state spostate nel capitolo Sicurezza	Le informazioni sulle politiche gestite vengono riviste e ampliate. Sia le informazioni sulle policy gestite che le informazioni sui ruoli collegati ai servizi sono state spostate nel capitolo Sicurezza.	15 marzo 2021
Severità rivista per i controlli CIS 1.1 e CIS 3.1 — CIS 3.14	La severità dei controlli CIS 1.1 e CIS 3.1 — CIS 3.14 è stata modificata in Bassa.	3 marzo 2021
È stato rimosso il controllo RDS.11	È stato rimosso il RDS.11 controllo dallo standard Foundational Security Best Practices.	3 marzo 2021

Integrazione aggiornata per Turbot	L'integrazione con Turbot viene aggiornata sia per l'invio che per la ricezione dei risultati .	26 febbraio 2021
Controlli aggiunti allo standard Foundational Security Best Practices	Sono stati aggiunti nuovi controlli per Amazon API Gateway (APIGateway.1), Amazon EC2 (EC2.9 and EC2.10), Amazon Elastic File System (EFS.2), Amazon OpenSearch Service (ES.2 and ES.3), Elastic Load Balancing ELB.6 () AWS Key Management Service e ()AWS KMS(). KMS.3	11 febbraio 2021
È stato aggiunto un `ProductArn` filtro opzionale all'API `DescribeProducts`	Il funzionamento dell'`DescribeProducts` API ora include un `ProductAr n` parametro opzionale. Il `ProductArn` parametro viene utilizzato per identific are l'integrazione specifica del prodotto per cui restituire i dettagli.	3 febbraio 2021
Nuova integrazione con Antivirus per Amazon S3 di Cloud Storage Security	L'integrazione con Antivirus for Amazon S3 invia i risultati della scansione antivirus al Security Hub CSPM come risultati.	27 gennaio 2021

È stato aggiornato il processo di calcolo del punteggio di sicurezza per gli account degli amministratori	Per un account amministratore, Security Hub CSPM utilizza un processo separato per calcolare il punteggio di sicurezza. Il nuovo processo garantisce che il punteggio includa controlli abilitati per gli account dei membri ma disabilitati per l'account amministratore.	21 gennaio 2021
Nuovi campi e oggetti nell'ASFF	È stato aggiunto un nuovo `Action` oggetto per tenere traccia delle azioni avvenute nei confronti di una risorsa. Sono stati aggiunti campi all'`AwsEc2NetworkInterface` oggetto per tenere traccia dei nomi DNS e degli indirizzi IP. È stato aggiunto un nuovo `AwsSsmPatchCompliance` oggetto ai dettagli della risorsa.	21 gennaio 2021
Aggiunti controlli allo standard Foundational Security Best Practices	Sono stati aggiunti nuovi controlli per Amazon CloudFront (CloudFront.1 tramite CloudFront.4), Amazon DynamoDB DynamoDB.1 (DynamoDB.3tramite), Elastic Load Balancing (ELB.3 tramite ELB.5), Amazon RDS (tramite) , Amazon Redshift (tramite eRDS.9) RDS.11 Redshift.1 e Amazon SNS (Redshift.3) Redshift.6. SNS.1	15 gennaio 2021

Lo stato del flusso di lavoro viene reimpostato in base allo stato del record o allo stato di conformità	Security Hub CSPM reimposta automaticamente lo stato del flusso di lavoro da `NOTIFIED` o `RESOLVED` verso `NEW` se un risultato archiviato viene reso attivo o se lo stato di conformità di un risultato cambia `PASSED` da,, o`FAILED`. `WARNING` `NOT_AVAILABLE` Queste modifiche indicano che sono necessarie ulteriori indagini.	7 gennaio 2021
`ProductFields` Informazioni aggiunte per i risultati basati sul controllo	Per i risultati generati dai controlli, sono state aggiunte informazioni sul contenuto dell'`ProductFields` oggetto nel AWS Security Finding Format (ASFF).	29 dicembre 2020
Aggiornamenti alle informazioni gestite	Modificato il titolo di insight 5. È stata aggiunta una nuova analisi, 32, che verifica la presenza di utenti IAM con attività sospette.	22 dicembre 2020
Aggiornamenti IAM.7 e controlli Lambda.1	Nello standard AWS Foundational Security Best Practices , sono stati aggiornati i parametri per IAM.7. Sono stati aggiornati il titolo e la descrizione di. Lambda.1	22 dicembre 2020

Integrazione estesa con ServiceNow ITSM	L'integrazione ServiceNow ITSM consente agli utenti di creare automaticamente incidenti o problemi quando viene ricevuto un risultato CSPM di Security Hub. Gli aggiornamenti a questi incidenti o problemi comportan o aggiornamenti dei risultati in Security Hub CSPM.	11 dicembre 2020
Nuova integrazione con AWS Audit Manager	Security Hub CSPM offre ora un'integrazione con AWS Audit Manager. L'integrazione consente all'Audit Manager di ricevere risultati basati sul controllo da Security Hub CSPM.	8 dicembre 2020
Nuova integrazione con Aqua Security Kube-bench	Security Hub CSPM ha aggiunto un'integrazione con Aqua Security. Kube-bench L'integrazione invia i risultati a Security Hub CSPM.	24 novembre 2020
Cloud Custodian è ora disponibile nelle regioni della Cina	L'integrazione con Cloud Custodian è ora disponibile nelle regioni Cina (Pechino) e Cina (Ningxia).	24 novembre 2020

BatchImportFindings ora può essere utilizzato per aggiornare campi aggiuntivi	In precedenza, non era possibile BatchImportFindings utilizzare per aggiornare i Types campi Confidence Criticality RelatedFindings ,Severity,, e. Ora, se questi campi non sono stati aggiornati daBatchUpdateFindings , possono essere aggiornati daBatchImportFindings . Una volta aggiornati daBatchUpdateFindings , non possono essere aggiornati daBatchImportFindings .	24 novembre 2020
Security Hub CSPM è ora integrato con AWS Organizations	I clienti possono ora gestire gli account dei membri utilizzando la configurazione dell'account Organizations. L'account di gestione dell'organizzazione e indica l'account amministratore CSPM di Security Hub, che determina quali account dell'organizzazione abilitare in Security Hub CSPM. La procedura di invito manuale può ancora essere utilizzata per gli account che non fanno parte di un'organizzazione.	23 novembre 2020

È stato rimosso il formato separato dell'elenco dei risultati per i controlli ad alto volume	L'elenco dei risultati per un controllo non utilizza più il formato della pagina Findings quando è presente un numero molto elevato di risultati.	19 novembre 2020
Integrazioni di terze parti nuove e aggiornate	Security Hub CSPM ora supporta le integrazioni con cloudtamer.io, 3CoreSec, Prowler e Kubernetes Security. StackRox IBM QRadar non invia più i risultati. Riceve solo risultati.	30 ottobre 2020
È stata aggiunta l'opzione per scaricare l'elenco dei risultati dalla pagina dei dettagli del controllo.	Nella pagina dei dettagli del controllo, una nuova opzione di download consente di scaricare l'elenco dei risultati in un file.csv. L'elenco scaricato rispetta tutti i filtri presenti nell'elenco. Se hai selezionato risultati specifici, l'elenco scaricato include solo tali risultati.	26 ottobre 2020
È stata aggiunta l'opzione per scaricare l'elenco dei controlli dalla pagina dei dettagli standard.	Nella pagina dei dettagli standard, una nuova opzione di download consente di scaricare l'elenco dei controlli in un file.csv. L'elenco scaricato rispetta tutti i filtri presenti nell'elenco. Se hai selezionato un controllo specifico, l'elenco scaricato include solo quel controllo.	26 ottobre 2020

Integrazioni con i partner nuove e aggiornate	Security Hub CSPM è ora integrato con. ThreatMod eler Sono state aggiornate le seguenti integrazioni con i partner in modo da rispecchi are i nuovi nomi di prodotto. Twistlock Enterprise Edition è ora Palo Alto Networks - Prisma Cloud Compute. Sempre di Palo Alto Networks, Demisto è ora Cortex XSOAR e Redlock è ora Prisma Cloud Enterprise.	23 ottobre 2020
Security Hub CSPM lanciato in Cina (Pechino) e Cina (Ningxia)	Security Hub CSPM è ora disponibile nelle regioni Cina (Pechino) e Cina (Ningxia).	21 ottobre 2020
Formato rivisto per gli attributi ASFF e le integrazioni di terze parti	Gli elenchi degli attributi ASFF e delle integrazioni dei partner ora utilizzano un formato basato su elenchi anziché su tabelle. La sintassi, gli attributi e la tassonomia dei tipi ASFF sono ora in argomenti separati.	15 ottobre 2020
Pagina dei dettagli standard riprogettata	La pagina dei dettagli standard per uno standard abilitato ora mostra un elenco a schede di controlli. Le schede filtrano l'elenco di controllo in base allo stato del controllo.	7 ottobre 2020

CloudWatch Eventi sostituiti con EventBridge	I riferimenti ad Amazon CloudWatch Events sono stati sostituiti con Amazon EventBridge.	1° ottobre 2020
Nuove integrazioni con Blue Hexagon for AWS, Alcide Audit e Palo Alto Networks. VM-Series	Security Hub CSPM è ora integrato con Blue Hexagon for AWS, Alcide KAudit e Palo Alto Networks. VM-Series Blue Hexagon for AWS e KAudit inviano i risultati al Security Hub CSPM. VM-Series riceve i risultati dal Security Hub CSPM.	30 settembre 2020
Oggetti di dettaglio delle risorse nuovi e aggiornati in ASFF	Sono stati aggiunti nuovi `Resources.Details` oggetti per `AwsApiGatewayRestApi` `AwsApiGatewayStage` ,`AwsApiGatewayV2Api` ,`AwsApiGatewayV2Stage` ,`AwsCertificateManagerCertificate` , `AwsElbLoadBalancer` `AwsIamGroup` , `eAwsRedshiftCluster` . Sono stati aggiunti dettagli `AwsIamAccessKey` agli oggetti `AwsIamRole` e. `AwsCloudFrontDistribution`	30 settembre 2020

Nuovo `ResourceRole` attributo per le risorse in ASFF per tracciare se una risorsa è un attore o un bersaglio.	L'`ResourceRole` attributo per le risorse indica se la risorsa è l'obiettivo dell'attività di ricerca o l'autore dell'attività di ricerca. I valori validi sono `ACTOR` e `TARGET`.	30 settembre 2020
È stato aggiunto AWS Systems Manager Patch Manager alle integrazioni di servizi disponibili AWS	AWS Systems Manager Patch Manager è ora integrato con Security Hub CSPM. Patch Manager invia i risultati a Security Hub CSPM quando le istanze della flotta di un cliente non sono conformi allo standard di conformità delle patch.	22 settembre 2020
Sono stati aggiunti nuovi controlli allo standard AWS Foundational Security Best Practices	Sono stati aggiunti nuovi controlli per i seguenti servizi: Amazon EC2 (EC2.7 and EC2.8), Amazon EMR (EMR.1), IAM ()IAM.8, Amazon RDS (attraver so)RDS.4 , RDS.8 Amazon S3 () e (S3.6e). AWS Secrets Manager SecretsManager.1 SecretsManager.2	15 settembre 2020
Nuove chiavi contestua li per la policy IAM per controllare l'accesso ai campi `BatchUpdateFindings`	Le policy IAM possono ora essere configurate per limitare l'accesso ai campi e ai valori dei campi durante l'utilizz o`BatchUpdateFindings` .	10 settembre 2020

Accesso esteso agli account `BatchUpdateFindings` per i membri	Per impostazione predefinita, gli account dei membri ora hanno lo stesso accesso agli `BatchUpdateFindings` account amministratore.	10 settembre 2020
Nuovi controlli per AWS KMS il Foundational Security Best Practices Standard	Sono stati aggiunti due nuovi controlli (KMS.1 e KMS.2) al Foundational Security Best Practices Standard. I nuovi controlli verificano se le politiche IAM limitano l'accesso alle AWS KMS azioni di decrittografia.	09 settembre 2020
Sono stati rimossi i risultati a livello di account per i controlli	Security Hub CSPM non genera più risultati a livello di account per un controllo. Vengono generati solo risultati a livello di risorsa.	1 settembre 2020
Nuovo oggetto in ASFF PatchSummary	Aggiunto l'`PatchSummary` oggetto all'ASFF. L'`PatchSummary` oggetto fornisce informazioni sulla conformità delle patch di una risorsa rispetto a uno standard di conformità selezionato.	1 settembre 2020

Pagina dei dettagli di controllo riprogettata	La pagina dei dettagli per i controlli è stata riprogett ata. L'elenco di ricerca dei controlli fornisce schede che consentono di filtrare rapidamente l'elenco in base allo stato di conformità. È inoltre possibile visualizz are rapidamente i risultati soppressi. Ogni voce fornisce l'accesso a dettagli aggiuntiv i sulla risorsa di ricerca, sulla AWS Config regola e sulle note di ricerca.	28 agosto 2020
Nuove opzioni di filtro per i risultati	Per trovare i filtri, puoi utilizzar e il filtro isnot per trovare i risultati per i quali il valore di un campo non è uguale al valore del filtro. È possibile utilizzare il comando non inizia con per trovare risultati per i quali un valore di campo non inizia con il valore di filtro specificato.	28 agosto 2020

Nuovi oggetti di dettaglio delle risorse in ASFF	Sono stati aggiunti nuovi `Resources.Details` oggetti per i seguenti tipi di risorse: `AwsDynamoDbTable` `AwsEc2Eip` ,`AwsIamPolicy` ,,`AwsIamUser` ,`AwsRdsDbCluster` ,`AwsRdsDbClusterSnapshot` , `AwsRdsDbSnapshot` `AwsSecretsManagerSecret`	18 agosto 2020
Nuova integrazione con RSA Archer	Security Hub CSPM è ora integrato con RSA Archer. RSA Archer riceve i risultati dal Security Hub CSPM.	18 agosto 2020
Nuovo campo Descrizione per AwsKmsKey	È stato aggiunto un `Description` campo all'`AwsKmsKey` oggetto sottostante`Resources.Details` .	18 agosto 2020
Campi aggiunti a AwsRdsDbInstance	Sono stati aggiunti diversi attributi all'`AwsRdsDbInstance` oggetto sottostante`Resources.Details` .	18 agosto 2020

Aggiornato il modo in cui Security Hub CSPM determina lo stato generale di un controllo	Per i controlli che non hanno risultati, lo stato è Nessun dato anziché Sconosciuto. Lo stato del controllo include sia i risultati a livello di account che a livello di risorsa. Lo stato del controllo non utilizza lo stato dei risultati del flusso di lavoro, tranne per ignorare i risultati soppressi.	13 agosto 2020
Aggiornato il modo in cui Security Hub CSPM calcola il punteggio di sicurezza per uno standard	Quando si calcola il punteggio di sicurezza per uno standard, Security Hub CSPM ora ignora i controlli con lo stato Nessun dato. Il punteggio di sicurezza è la proporzione dei controlli passati rispetto ai controlli abilitati, esclusi i controlli senza dati.	13 agosto 2020
Nuova opzione per abilitare automaticamente nuovi controlli negli standard abilitati	È stata aggiunta un'opzione Impostazioni per abilitare automaticamente i nuovi controlli negli standard abilitati. Puoi anche utilizzare l'operazione `UpdateSecurityHubConfiguration` API per configurare questa opzione.	31 luglio 2020

Nuovi controlli per lo standard PCI DSS (Payment Card Industry Data Security Standard)	Aggiunti nuovi controlli allo standard PCI DSS. Gli identificatori dei nuovi controlli sono PCI.DMS.1,,, 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 e. PCI.SSM.3	29 luglio 2020
Controlli nuovi e aggiornati per lo standard Foundational Security Best Practices	Aggiunti nuovi controlli allo standard Foundational Security Best Practices. Gli identificatori dei nuovi controlli sono AutoScaling.1,, DMS.1, EC2.4 EC2.6 S3.5, e. SSM.3 È stato aggiornato il titolo ACM.1 e modificato il valore del `daysToExpiration` parametro portandolo a 30.	29 luglio 2020
Nuovo `Vulnerabilities` oggetto nell'ASFF	È stato aggiunto l'`Vulnerabilities` oggetto, che fornisce informazioni sulle vulnerabilità associate alla scoperta.	1 luglio 2020
Nuovi `Resource.Details` oggetti nei gruppi ASFF for Auto Scaling, nei volumi EC2 e nei VPC EC2	Sono stati aggiunti gli oggetti`AwsAutoScalingAutoScalingGroup` , `AWSEc2Volume` e a. `AwsEc2Vpc` `Resource.Details`	1 luglio 2020
Nuovo `NetworkPath` oggetto nell'ASFF	È stato aggiunto l'`NetworkPath` oggetto, che fornisce informazioni su un percorso di rete correlato al risultato.	1 luglio 2020

Risolvi automaticamente i risultati quando `Compliance.Status` è `PASSED`	Per i risultati dei controlli, in caso `Compliance.Status` affermativo `PASSED`, Security Hub CSPM si imposta `Workflow.Status` automaticamente su. `RESOLVED`	24 giugno 2020
AWS Command Line Interface esempi	AWS CLI Sintassi ed esempi aggiunti per diverse attività CSPM di Security Hub. Include l'abilitazione di Security Hub CSPM, la gestione degli approfondimenti, la gestione degli standard e dei controlli, la gestione delle integrazioni dei prodotti e la disabilitazione di Security Hub CSPM.	24 giugno 2020
Nuovo attributo nell'ASFF `Severity.Original`	Aggiunto l'attributo `Severity.Original` che corrisponde alla gravità originale del provider di risultati. Sostituisce l'attributo `Severity.Product` obsoleto.	20 maggio 2020
Nuovo `Compliance.StatusReasons` oggetto nell'ASFF per i dettagli sullo stato di un controllo	Aggiunto l'oggetto `Compliance.StatusReasons` che fornisce un contesto aggiuntivo per lo stato corrente di un controllo.	20 maggio 2020

Nuovo standard AWS Foundational Security Best Practices	È stato aggiunto il nuovo standard AWS Foundational Security Best Practices, che è un insieme di controlli che rilevano quando gli account e le risorse distribuiti si discostano dalle migliori pratiche di sicurezza.	22 aprile 2020
Nuova opzione di console per aggiornare lo stato del flusso di lavoro per una ricerca	Aggiunte informazioni per l'utilizzo della console o dell'API Security Hub per impostare lo stato del flusso di lavoro per i risultati.	16 aprile 2020
Nuova `BatchUpdateFindings` API per gli aggiornamenti dei risultati da parte dei clienti	Aggiunte informazioni sull'utilizzo di `BatchUpdateFindings` per aggiornare le informazioni relative al processo di indagine di un risultato. `BatchUpdateFindings` sostituisce `UpdateFindings` che è obsoleto.	16 aprile 2020

Aggiornamenti al AWS Security Finding Format (ASFF)	Aggiunti diversi nuovi tipi di risorse. Aggiunto un nuovo attributo `Label` all'oggetto `Severity`. `Label` è destinato a sostituire il campo `Normalized` . Aggiunto un nuovo oggetto `Workflow` per tracciare il processo di un'indagine su un risultato . `Workflow` contiene un attributo `Status` che sostituisce l'attributo `WorkflowsTate` esistente.	12 marzo 2020
Aggiornamenti alla pagina delle integrazioni	Aggiornato per riflettere le modifiche apportate alla pagina Integrazioni. Per ogni integrazione, la pagina mostra ora la categoria di integrazione e se ogni integrazione invia o riceve i risultati da Security Hub CSPM. Fornisce inoltre i passaggi specifici necessari per abilitare ogni integrazione.	26 febbraio 2020
Nuove integrazioni di prodotti di terze parti	Sono state aggiunte le seguenti nuove integrazioni di prodotto: Cloud Custodian , FireEye Helix, Forcepoint CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security e Cognito Detect. Vectra.ai	21 febbraio 2020

Nuovo standard di sicurezza per il Payment Card Industry Data Security Standard (PCI DSS)	È stato aggiunto lo standard di sicurezza Security Hub CSPM per il Payment Card Industry Data Security Standard (PCI DSS). Quando questo standard è abilitato, Security Hub CSPM esegue controlli automatici rispetto ai controlli relativi ai requisiti PCI DSS.	13 febbraio 2020
Aggiornamenti al AWS Security Finding Format (ASFF)	Aggiunto un campo per i requisiti correlati ai controlli degli standard. Aggiunti nuovi tipi di risorse e nuovi dettagli delle risorse. L'ASFF ora ti permette anche di offrire fino a 32 risorse.	05 febbraio 2020
Nuova opzione per disabilitare i singoli controlli standard di sicurezza	Aggiunte informazioni su come verificare se ogni singolo controllo degli standard di sicurezza è abilitato.	15 gennaio 2020
Aggiornamenti ai concetti CSPM di Security Hub	Sono state aggiornate alcune descrizioni e aggiunto nuovi termini ai concetti CSPM di Security Hub.	21 settembre 2019
AWS Versione di disponibilità generale di Security Hub CSPM	Aggiornamenti dei contenuti per riflettere i miglioramenti apportati a Security Hub CSPM durante il periodo beta.	25 giugno 2019
Aggiunti passaggi di correzione per i controlli di AWS CIS Foundations	Sono stati aggiunti passaggi di correzione agli standard di sicurezza supportati in AWS Security Hub CSPM.	15 aprile 2019

versione beta di AWS Security Hub CSPM	Pubblicata la versione beta della AWS Security Hub CSPM User Guide.	18 novembre 2018

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.