Panduan GuardDuty Pengguna Amazon

Amazon GuardDuty



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

Amazon GuardDuty: Panduan GuardDuty Pengguna Amazon

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu GuardDuty? 1
Fitur GuardDuty 2
Kepatuhan PCI DSS 7
Harga di GuardDuty 7
Menggunakan uji GuardDuty coba gratis 30 hari 8
Menggunakan Perlindungan Malware untuk S3 dengan Tingkat Gratis 10
Mengakses GuardDuty 10
Konsep dan istilah kunci 12
Memulai 17
Sebelum Anda mulai 17
Langkah 1: Aktifkan Amazon GuardDuty 19
Langkah 2: Menghasilkan temuan sampel dan menjelajahi operasi dasar 22
Langkah 3: Konfigurasikan GuardDuty temuan ekspor ke bucket Amazon S3 23
Langkah 4: Siapkan peringatan GuardDuty pencarian melalui SNS 28
Langkah selanjutnya 32
Sumber data dasar 33
AWS CloudTrail acara manajemen 33
Bagaimana GuardDuty menangani AWS CloudTrail peristiwa global 34
Log Alur VPC 35
Log kueri DNS Route53 Resolver 36
Deteksi Ancaman yang Diperpanjang 37
Contoh skenario ancaman urutan serangan 37
Cara kerja Deteksi Ancaman yang Diperluas 38
Mengaktifkan rencana perlindungan untuk memaksimalkan deteksi ancaman 39
Mendeteksi urutan serangan di cluster Amazon EKS 40
Mendeteksi urutan serangan di bucket Amazon S3 41
Mendeteksi urutan serangan di cluster Amazon ECS 42
Mendeteksi urutan serangan di grup instans Amazon EC2 42
Mendeteksi urutan serangan yang melibatkan beban kerja AI 43
Deteksi Ancaman Diperpanjang di GuardDuty konsol 44
Memahami dan mengelola temuan urutan serangan 44
Sumber daya tambahan 45
Rencana perlindungan 46
Ikhtisar 46

Mengkonfigurasi semua rencana perlindungan 46
Auto-enable pilihan 47
Konfigurasi Runtime Monitoring 47
Kendala dua arah 48
Statistik organisasi 49
Integrasi halaman akun 49
Perlindungan AI 50
Bagaimana AI Protection bekerja 51
Harga untuk Perlindungan AI 52
Deteksi ancaman tambahan untuk beban kerja AI 53
Mengaktifkan Perlindungan AI di lingkungan multi-akun 53
Mengaktifkan Perlindungan AI untuk akun mandiri 57
Perlindungan EKS 59
Log audit EKS di Perlindungan EKS 60
Mengaktifkan Perlindungan EKS di lingkungan multi-akun 61
Mengaktifkan Perlindungan EKS untuk akun mandiri 68
Perlindungan S3 70
AWS CloudTrail peristiwa data untuk S3 71
Cara GuardDuty menggunakan peristiwa CloudTrail data untuk S3 71
GuardDuty menggunakan peristiwa CloudTrail data untuk S3 untuk urutan serangan 72
Mengaktifkan Perlindungan S3 di lingkungan beberapa akun 72
Mengaktifkan Perlindungan S3 untuk akun mandiri 79
Pemantauan Runtime 81
Cara kerjanya 82
Pemberdayaan 83
Terapkan ke Amazon EKS 84
Terapkan ke Amazon EC2 86
Terapkan ke Amazon ECS di Fargate 88
Konektivitas agen 89
Melacak cakupan Pemantauan Runtime 91
Uji coba gratis 30 hari 92
Saya menggunakan masa GuardDuty percobaan atau saya tidak pernah mengaktifkan EKS Runtime Monitoring 92
Saya mengaktifkan EKS Runtime Monitoring sebelum peluncuran Runtime Monitoring 93
Prasyarat 94
Untuk contoh EC2 94

Untuk ECS-EC2 Bottlerocket 98
Untuk cluster Fargate (khusus ECS) 102
Untuk kluster EKS 108
Arsitektur CPU, sistem operasi, dan versi kernel yang didukung 111
Mengaktifkan Runtime Monitoring 112
Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun 113
Mengaktifkan Runtime Monitoring untuk akun mandiri 116
Mengelola agen GuardDuty keamanan 116
Agen otomatis pada sumber daya Amazon EC2 117
Manajemen agen manual untuk sumber daya Amazon EC2 130
Agen otomatis pada sumber daya ECS-EC2 Bottlerocket 146
Agen otomatis pada sumber daya Fargate (khusus Amazon ECS) 147
Agen otomatis di sumber daya Amazon EKS 183
Manajemen agen manual untuk klaster Amazon EKS 221
Konfigurasikan parameter add-on EKS 230
Memvalidasi konfigurasi titik akhir VPC 233
Masalah cakupan runtime dan pemecahan masalah 235
Cakupan dan pemecahan masalah untuk sumber daya Amazon EC2 236
Cakupan dan pemecahan masalah untuk Bottlerocket ECS-EC2 252
Cakupan dan pemecahan masalah untuk klaster Amazon ECS 259
Cakupan dan pemecahan masalah untuk klaster Amazon EKS 275
Menyiapkan CPU dan pemantauan memori 291
Menggunakan VPC bersama 292
Cara kerjanya 293
Prasyarat 295
Menggunakan IAc dengan agen otomatis 295
Ikhtisar grafik ketergantungan sumber daya IAc 296
Masalah umum - Menghapus sumber daya di IAc 296
Jenis acara runtime yang dikumpulkan 298
Memproses acara 298
Acara kontainer 300
AWS Fargate (Hanya Amazon ECS) peristiwa tugas 301
Acara pod Kubernetes 302
Acara Sistem Nama Domain (DNS) 302
Buka acara 303
Memuat acara modul 303

Acara Mprotect 304
Acara gunung 304
Tautkan acara 304
Acara Symlink 305
Acara Dup 305
Acara peta memori 306
Acara soket 306
Connect event 307
Memproses acara VM Readv 308
Proses acara VM Writev 308
Process trace (Ptrace) peristiwa 309
Mengikat acara 309
Dengarkan acara 310
Ganti nama acara 310
Mengatur peristiwa ID pengguna (UID) 311
Acara Chmod 311
Agen hosting repositori Amazon ECR GuardDuty 311
Repo ECR untuk EKS v1.16.0 - 1.8.1 (eks.build.2) 312
Repo ECR untuk versi EKS `1.8.1.eks.build.1` 317
Repositori ECR untuk agen keamanan di (hanya AWS Fargate Amazon ECS) 320
Repositori ECR untuk agen keamanan di Bottlerocket ECS-EC2 324
Agen keamanan di host yang sama 328
Gambaran umum 328
Dampak 328
Bagaimana GuardDuty menangani banyak agen 328
Pemantauan Runtime EKS 329
Mengkonfigurasi EKS Runtime Monitoring untuk lingkungan multi-akun (API) 330
Mengkonfigurasi EKS Runtime Monitoring untuk akun mandiri (API) 371
Bermigrasi dari Pemantauan Runtime EKS ke Pemantauan Runtime 379
GuardDuty versi rilis agen keamanan 383
Sumber daya tambahan - langkah selanjutnya 424
Menonaktifkan, menghapus instalasi, dan pembersihan sumber daya 425
Menghapus instalan agen keamanan secara manual untuk sumber daya Amazon EC2 427
Menghapus instalan agen keamanan untuk sumber daya ECS-EC2 Bottlerocket 429
Membersihkan sumber daya agen keamanan 429
Perlindungan Malware untuk EC2 432

Membandingkan pemindaian GuardDuty-initiated malware dan pemindaian On-demand malware 433
Cara GuardDuty memindai volume EBS untuk deteksi malware 436
Volume EBS yang didukung 437
Ubah ID kunci KMS default 438
Mengatur retensi snapshot dan cakupan pemindaian EC2 439
Retensi snapshot 439
Opsi pindai dengan tag yang ditentukan pengguna 441
`GuardDutyExcludedTag` global 445
GuardDuty-initiated pemindaian malware 445
Uji coba gratis 30 hari 446
Mengaktifkan pemindaian GuardDuty-initiated malware di lingkungan beberapa akun 447
Mengaktifkan pemindaian GuardDuty-initiated malware untuk akun mandiri 458
Temuan yang memanggil pemindaian GuardDuty-initiated malware 459
On-demand pemindaian malware 462
Cara kerja pemindaian On-demand malware 463
Memulai pemindaian On-demand malware 464
Re-scanning instans Amazon EC2 yang sebelumnya dipindai 466
Memantau status dan hasil pemindaian malware 467
GuardDuty akun layanan 469
Kuota dalam Perlindungan Malware untuk EC2 472
Perlindungan Malware untuk S3 477
Harga dan biaya penggunaan 479
Meninjau biaya penggunaan 480
Cara kerjanya 481
Gambaran umum 481
Izin peran IAM 481
Penandaan opsional objek berdasarkan hasil pemindaian 481
Proses setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk ember 482
Kemampuan Perlindungan Malware untuk S3 484
(Opsional) Memulai dengan Perlindungan Malware hanya untuk S3 (konsol) 486
Mengkonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda 487
Mengaktifkan Perlindungan Malware untuk deteksi ancaman S3 untuk bucket Anda 488
Izin peran IAM 494
Memecahkan masalah kesalahan izin peran IAM 500
Langkah-langkah setelah mengaktifkan Perlindungan Malware untuk S3 501

On-demand Pemindaian malware S3 502
Prasyarat 502
Mulai pemindaian malware sesuai permintaan 503
Menggunakan kontrol akses berbasis tag (TBAC) 504
Menambahkan TBAC pada sumber daya bucket S3 504
Lihat dan pahami status bucket yang dilindungi 507
Memantau pemindaian objek S3 508
Status pemindaian potensial objek S3 dan status hasil 508
Menggunakan Amazon EventBridge 512
Menggunakan Tag Objek S3 522
Menggunakan CloudWatch alarm dan metrik 523
Pemecahan Masalah 527
Memecahkan masalah status paket Perlindungan Malware 527
Memecahkan masalah pemindaian malware sesuai permintaan 531
Mengedit paket Perlindungan Malware untuk bucket yang dilindungi 531
Menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi 533
Dukungan fitur Amazon S3 534
Perlindungan Malware untuk kuota S3 541
Perlindungan Malware untuk AWS Backup 544
Gambaran umum 544
Cara kerjanya 546
Gambaran umum 544
Peran IAM Diperlukan untuk Pemindaian 549
Meninjau status dan hasil pemindaian Sumber Daya 549
Meninjau temuan yang dihasilkan 549
Izin Peran IAM 550
Peran pelanggan disediakan untuk pemindaian malware 550
Detail tentang izin 550
Mengamankan Peran 551
Bagaimana Perlindungan GuardDuty Malware menggunakan hibah di AWS KM 552
GuardDuty Konteks Enkripsi Perlindungan Malware 552
Izin dan kebijakan kepercayaan untuk peran 553
Memulai secara mandiri 557
Langkah-langkah untuk memulai dengan Perlindungan Malware untuk Backup 557
Memulai pemindaian sesuai permintaan 558
Konsol 558

API/CLI 559
Memantau status dan hasil pemindaian malware 559
Perlindungan Malware untuk Kuota Cadangan 568
Perlindungan RDS 572
Basis data yang didukung 574
Aktivitas login RDS 575
Aktivitas data RDS 576
Mengaktifkan Perlindungan RDS di lingkungan multi-akun 576
Mengaktifkan Perlindungan RDS untuk akun mandiri 585
Memecahkan masalah pemantauan Perlindungan RDS 586
Penyimpanan RDS penuh 586
Versi yang tidak didukung pada database utama untuk RDS untuk PostgreSQL 587
Pertimbangan keamanan tambahan 587
Perlindungan Lambda 589
Pemantauan Aktivitas Jaringan Lambda 590
Mengaktifkan Perlindungan Lambda di lingkungan multi-akun 590
Mengaktifkan Perlindungan Lambda untuk akun mandiri 597
Investigasi - Pratinjau 599
Jenis analisis 599
Cross-Region kesimpulan 600
Prasyarat 601
Model akses untuk akun administrator dan anggota 602
Membuat investigasi 603
Melihat hasil investigasi 605
Menafsirkan hasil investigasi 607
Investigasi daftar 608
Aturan Deteksi Kustom 611
Cara Kerja Aturan Deteksi Kustom 612
Sumber data dan sinyal 612
Modus 613
Menemukan agregasi 613
Bidang acara yang disunting 614
Aturan Deteksi Kustom yang Tersedia 615
Melihat logika deteksi aturan 615
Fungsi yang digunakan dalam logika deteksi 616
Mengelola Aturan Deteksi Kustom 618

Daftar aturan yang tersedia 618
Melihat status aturan 619
Operasi massal 619
Lari kering 620
Hidup 621
Menonaktifkan aturan 622
Mengelola Aturan Deteksi Kustom di lingkungan multi-akun 623
Konfigurasi organisasi 623
Menjalankan kedua mode untuk aturan yang sama 624
Contoh: Menerapkan aturan dalam mode dry run ke semua akun anggota 625
Menerapkan setiap aturan di seluruh organisasi 625
Mengelola beberapa akun 627
Akun administrator dan hubungan akun anggota 628
Status hubungan anggota 633
Mengelola akun dengan AWS Organizations 634
Pertimbangan dan rekomendasi 635
Izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty 637
Menunjuk akun administrator yang didelegasikan GuardDuty 638
Menyetel preferensi aktifkan otomatis organisasi 640
Menambahkan anggota ke organisasi 644
(Opsional) Aktifkan paket perlindungan untuk akun anggota yang ada 646
Terus mengelola akun anggota Anda dalam GuardDuty 647
Penangguhan GuardDuty untuk akun anggota 648
Memutuskan (menghapus) akun anggota dari akun administrator 650
Menghapus akun anggota dari organisasi GuardDuty 651
Mengubah akun GuardDuty administrator yang didelegasikan 653
Mengelola akun menggunakan kebijakan organisasi 655
Prasyarat 656
Bagaimana kebijakan organisasi bekerja 657
Membuat kebijakan di konsol 659
Meninjau dampak kebijakan sebelum Anda menerapkannya 660
Pertimbangan dan batasan 662
Mengelola akun dengan undangan 664
Menambahkan akun dengan undangan 665
Mengkonsolidasikan akun administrator di bawah satu organisasi 670
GuardDuty pertimbangan untuk opsi Ekspor CSV di akun 672

Tipe temuan 674
Tipe temuan EC2 674
Backdoor:EC2/C&CActivity.B 676
Backdoor:EC2/C&CActivity.B!DNS 677
Backdoor:EC2/DenialOfService.Dns 678
Backdoor:EC2/DenialOfService.Tcp 679
Backdoor:EC2/DenialOfService.Udp 679
Backdoor:EC2/DenialOfService.UdpOnTcpPorts 680
Backdoor:EC2/DenialOfService.UnusualProtocol 681
Backdoor:EC2/Spambot 681
Behavior:EC2/NetworkPortUnusual 682
Behavior:EC2/TrafficVolumeUnusual 682
CryptoCurrency:EC2/BitcoinTool.B 683
CryptoCurrency:EC2/BitcoinTool.B!DNS 684
DefenseEvasion:EC2/UnusualDNSResolver 684
DefenseEvasion:EC2/UnusualDoHActivity 685
DefenseEvasion:EC2/UnusualDoTActivity 685
Impact:EC2/AbusedDomainRequest.Reputation 686
Impact:EC2/BitcoinDomainRequest.Reputation 687
Impact:EC2/MaliciousDomainRequest.Reputation 687
Impact:EC2/MaliciousDomainRequest.Custom 688
Impact:EC2/PortSweep 689
Impact:EC2/SuspiciousDomainRequest.Reputation 689
Impact:EC2/WinRMBruteForce 690
Recon:EC2/PortProbeEMRUnprotectedPort 690
Recon:EC2/PortProbeUnprotectedPort 691
Recon:EC2/Portscan 692
Trojan:EC2/BlackholeTraffic 693
Trojan:EC2/BlackholeTraffic!DNS 693
Trojan:EC2/DGADomainRequest.B 694
Trojan:EC2/DGADomainRequest.C!DNS 695
Trojan:EC2/DNSDataExfiltration 695
Trojan:EC2/DriveBySourceTraffic!DNS 696
Trojan:EC2/DropPoint 697
Trojan:EC2/DropPoint!DNS 697
Trojan:EC2/PhishingDomainRequest!DNS 698

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom 698
UnauthorizedAccess:EC2/MetadataDNSRebind 699
UnauthorizedAccess:EC2/RDPBruteForce 700
UnauthorizedAccess:EC2/SSHBruteForce 700
UnauthorizedAccess:EC2/TorClient 702
UnauthorizedAccess:EC2/TorRelay 702
Tipe temuan IAM 703
CredentialAccess:IAMUser/AnomalousBehavior 704
CredentialAccess:IAMUser/CompromisedCredentials 705
DefenseEvasion:IAMUser/AnomalousBehavior 705
DefenseEvasion:IAMUser/BedrockLoggingDisabled 706
Discovery:IAMUser/AnomalousBehavior 706
Exfiltration:IAMUser/AnomalousBehavior 707
Impact:IAMUser/AnomalousBehavior 708
InitialAccess:IAMUser/AnomalousBehavior 709
PenTest:IAMUser/KaliLinux 709
PenTest:IAMUser/ParrotLinux 710
PenTest:IAMUser/PentooLinux 710
Persistence:IAMUser/AnomalousBehavior 711
Policy:IAMUser/RootCredentialUsage 712
Policy:IAMUser/ShortTermRootCredentialUsage 712
PrivilegeEscalation:IAMUser/AnomalousBehavior 713
Recon:IAMUser/MaliciousIPCaller 714
Recon:IAMUser/MaliciousIPCaller.Custom 714
Recon:IAMUser/TorIPCaller 715
Stealth:IAMUser/CloudTrailLoggingDisabled 715
Stealth:IAMUser/PasswordPolicyChange 716
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B 716
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS 717
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS 719
UnauthorizedAccess:IAMUser/MaliciousIPCaller 720
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom 721
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS 721
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS 723
UnauthorizedAccess:IAMUser/TorIPCaller 724
Jenis pencarian urutan serangan 725

AttackSequence:EKS/CompromisedCluster 726
AttackSequence:ECS/CompromisedCluster 727
AttackSequence:EC2/CompromisedInstanceGroup 727
AttackSequence:IAM/CompromisedCredentials 729
AttackSequence:S3/CompromisedData 730
Jenis pencarian Aturan Deteksi Kustom 730
Aturan Deteksi Kustom untuk AWS CloudTrail acara manajemen 731
Aturan Deteksi Kustom untuk Pemantauan Runtime 735
Jenis temuan perlindungan S3 741
Discovery:S3/AnomalousBehavior 742
Discovery:S3/MaliciousIPCaller 743
Discovery:S3/MaliciousIPCaller.Custom 743
Discovery:S3/TorIPCaller 744
Exfiltration:S3/AnomalousBehavior 744
Exfiltration:S3/MaliciousIPCaller 745
Impact:S3/AnomalousBehavior.Delete 746
Impact:S3/AnomalousBehavior.Permission 747
Impact:S3/AnomalousBehavior.Write 747
Impact:S3/MaliciousIPCaller 748
PenTest:S3/KaliLinux 749
PenTest:S3/ParrotLinux 749
PenTest:S3/PentooLinux 750
Policy:S3/AccountBlockPublicAccessDisabled 750
Policy:S3/BucketAnonymousAccessGranted 751
Policy:S3/BucketBlockPublicAccessDisabled 752
Policy:S3/BucketPublicAccessGranted 752
Stealth:S3/ServerAccessLoggingDisabled 753
UnauthorizedAccess:S3/MaliciousIPCaller.Custom 754
UnauthorizedAccess:S3/TorIPCaller 754
Jenis penemuan Perlindungan EKS 755
CredentialAccess:Kubernetes/MaliciousIPCaller 757
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom 757
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess 758
CredentialAccess:Kubernetes/TorIPCaller 759
DefenseEvasion:Kubernetes/MaliciousIPCaller 759
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom 760

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess 761
DefenseEvasion:Kubernetes/TorIPCaller 761
Discovery:Kubernetes/MaliciousIPCaller 762
Discovery:Kubernetes/MaliciousIPCaller.Custom 763
Discovery:Kubernetes/SuccessfulAnonymousAccess 764
Discovery:Kubernetes/TorIPCaller 764
Execution:Kubernetes/ExecInKubeSystemPod 765
Impact:Kubernetes/MaliciousIPCaller 766
Impact:Kubernetes/MaliciousIPCaller.Custom 766
Impact:Kubernetes/SuccessfulAnonymousAccess 767
Impact:Kubernetes/TorIPCaller 768
Persistence:Kubernetes/MaliciousIPCaller 768
Persistence:Kubernetes/MaliciousIPCaller.Custom 769
Persistence:Kubernetes/SuccessfulAnonymousAccess 770
Persistence:Kubernetes/TorIPCaller 770
Policy:Kubernetes/AdminAccessToDefaultServiceAccount 771
Policy:Kubernetes/AnonymousAccessGranted 772
Policy:Kubernetes/ExposedDashboard 772
Policy:Kubernetes/KubeflowDashboardExposed 773
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed 773
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated 774
Execution:Kubernetes/AnomalousBehavior.ExecInPod 775
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer 776
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount 777
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed 778
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated 779
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked 780
Jenis penemuan Runtime Monitoring 781
Menemukan tipe yang dihasilkan Runtime Monitoring secara default 781
Menemukan jenis yang memerlukan Aturan Deteksi Kustom 819
Perlindungan Malware untuk jenis pencarian EC2 821
Execution:EC2/MaliciousFile 822
Execution:ECS/MaliciousFile 823
Execution:Kubernetes/MaliciousFile 823

Execution:Container/MaliciousFile 824
Execution:EC2/SuspiciousFile 824
Execution:ECS/SuspiciousFile 825
Execution:Kubernetes/SuspiciousFile 825
Execution:Container/SuspiciousFile 826
Perlindungan Malware untuk tipe pencarian S3 827
Object:S3/MaliciousFile 827
Perlindungan Malware untuk jenis pencarian Backup 828
Execution:EC2/MaliciousFile!Snapshot 828
Execution:EC2/MaliciousFile!AMI 829
Execution:EC2/MaliciousFile!RecoveryPoint 829
Execution:S3/MaliciousFile!RecoveryPoint 829
Jenis temuan Perlindungan RDS 830
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin 831
CredentialAccess:RDS/AnomalousBehavior.FailedLogin 832
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce 833
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin 834
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin 834
Discovery:RDS/MaliciousIPCaller 835
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin 835
CredentialAccess:RDS/TorIPCaller.FailedLogin 836
Discovery:RDS/TorIPCaller 837
Exfiltration:RDS/AnomalousBehavior 837
Impact:RDS/AnomalousBehavior.Drop 839
Impact:RDS/AnomalousBehavior.Delete 840
Exfiltration:RDS/MaliciousIPCaller 841
Exfiltration:RDS/TorIPCaller 842
Impact:RDS/MaliciousIPCaller 843
Impact:RDS/TorIPCaller 843
Jenis temuan Perlindungan Lambda 844
Backdoor:Lambda/C&CActivity.B 845
CryptoCurrency:Lambda/BitcoinTool.B 845
Trojan:Lambda/BlackholeTraffic 846
Trojan:Lambda/DropPoint 847
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom 847
UnauthorizedAccess:Lambda/TorClient 848

UnauthorizedAccess:Lambda/TorRelay 848
Jenis penemuan Perlindungan AI 849
Impact:IAMUser/AnomalousModelInvocation 849
Impact:IAMUser/CostHarvesting 851
Impact:IAMUser/PromptInjection.Direct 852
Tipe temuan yang sudah dihentikan 855
PrivilegeEscalation:Kubernetes/PrivilegedContainer 856
Persistence:Kubernetes/ContainerWithSensitiveMount 856
Exfiltration:S3/ObjectRead.Unusual 857
Impact:S3/PermissionsModification.Unusual 858
Impact:S3/ObjectDelete.Unusual 858
Discovery:S3/BucketEnumeration.Unusual 859
Persistence:IAMUser/NetworkPermissions 860
Persistence:IAMUser/ResourcePermissions 861
Persistence:IAMUser/UserPermissions 861
PrivilegeEscalation:IAMUser/AdministrativePermissions 862
Recon:IAMUser/NetworkPermissions 863
Recon:IAMUser/ResourcePermissions 864
Recon:IAMUser/UserPermissions 865
ResourceConsumption:IAMUser/ComputeResources 865
Stealth:IAMUser/LoggingConfigurationModified 866
UnauthorizedAccess:IAMUser/ConsoleLogin 867
UnauthorizedAccess:EC2/TorIPCaller 868
Backdoor:EC2/XORDDOS 868
Behavior:IAMUser/InstanceLaunchUnusual 869
CryptoCurrency:EC2/BitcoinTool.A 869
UnauthorizedAccess:IAMUser/UnusualASNCaller 869
GuardDuty menemukan jenis dengan sumber daya yang berpotensi terkena dampak 870
GuardDuty jenis temuan aktif 870
Memahami dan menghasilkan temuan 896
GuardDuty menemukan format 897
Tujuan Ancaman 898
GuardDuty mesin pemindai deteksi malware 902
Sampel temuan 902
Menghasilkan temuan sampel melalui GuardDuty konsol atau API 903
GuardDuty Temuan uji 904

Pertimbangan-pertimbangan 905
GuardDuty temuan skrip tester dapat menghasilkan 906
Langkah 1 - Prasyarat 908
Langkah 2 - Menyebarkan sumber daya AWS 909
Langkah 3 - Jalankan skrip penguji 911
Langkah 4 - Bersihkan sumber daya AWS tes 913
Memecahkan masalah umum 913
Halaman temuan di GuardDuty konsol 915
Menavigasi halaman Temuan 916
Tingkat keparahan temuan 918
Tingkat keparahan kritis 918
Tingkat keparahan tinggi 919
Tingkat keparahan sedang 919
Tingkat keparahan rendah 920
Detail temuan 920
Menemukan ikhtisar 921
Sumber daya 922
Detail pencarian urutan serangan 929
Aturan Deteksi Kustom menemukan detail 936
Rincian pengguna database RDS (DB) 938
Detail temuan Pemantauan Runtime 939
Detail pemindaian volume EBS 941
Perlindungan Malware untuk detail pencarian EC2 942
Detail temuan Perlindungan Malware untuk S3 943
Tindakan 944
Aktor atau Target 946
Detail geolokasi 947
Informasi tambahan 947
Bukti 947
Perilaku anomali 948
GuardDuty menemukan agregasi 953
Mengelola GuardDuty temuan 955
GuardDuty Dasbor ringkasan 956
Ikhtisar 957
Temuan 958
Jenis temuan yang paling umum 959

Temuan berdasarkan tingkat keparahan 959
Akun dengan sebagian besar temuan 959
Sumber daya dengan temuan 959
Temuan yang paling tidak terjadi 960
Cakupan rencana perlindungan 961
Penyaringan temuan GuardDuty 961
Membuat dan menyimpan set filter di GuardDuty konsol 962
Membuat dan menyimpan set filter dengan menggunakan GuardDuty API dan CLI 964
Metadata Siklus Hidup 966
Filter properti di GuardDuty 967
Aturan penekanan 1001
Menggunakan aturan penindasan dengan Deteksi Ancaman yang Diperluas 1001
Kasus penggunaan umum untuk aturan penekanan dan contoh 1002
Membuat aturan penekanan 1005
Memperbarui aturan penekanan 1010
Menghapus aturan penekanan 1013
Metrik aturan penekanan 1014
Daftar entitas dan daftar alamat IP 1015
Memahami daftar entitas dan daftar alamat IP 1016
Pertimbangan penting untuk daftar GuardDuty 1017
Format daftar 1018
Memahami status daftar 1027
Menyiapkan prasyarat untuk daftar entitas dan daftar alamat IP 1028
Menambahkan dan mengaktifkan daftar entitas atau daftar IP 1030
Memperbarui daftar entitas atau daftar alamat IP 1036
De-activating daftar entitas atau daftar alamat IP 1041
Menghapus daftar entitas atau daftar alamat IP 1043
Mengekspor temuan yang dihasilkan ke Amazon S3 1046
Pertimbangan-pertimbangan 1047
Langkah 1 - Izin diperlukan untuk mengekspor temuan 1048
Langkah 2 - Melampirkan kebijakan ke kunci KMS Anda 1048
Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3 1050
Langkah 4 - Mengekspor temuan ke bucket S3 (Konsol) 1054
Langkah 5 — Frekuensi untuk mengekspor temuan 1055
Memproses temuan dengan EventBridge 1056
EventBridge frekuensi pemberitahuan di GuardDuty 1057

Siapkan topik dan titik akhir Amazon SNS 1057
Menggunakan EventBridge dengan GuardDuty 1059
Membuat EventBridge aturan 1061
EventBridge aturan untuk lingkungan multi-akun 1068
Memahami CloudWatch Log dan alasan melewatkan sumber daya 1069
Mengaudit CloudWatch Log dalam Per GuardDuty lindungan Malware untuk EC2 1069
GuardDuty Perlindungan Malware untuk retensi log EC2 1071
Alasan melewatkan sumber daya 1072
Melaporkan hasil pemindaian malware EC2 positif palsu 1078
Melaporkan hasil pemindaian objek S3 positif palsu 1079
Melaporkan hasil pemindaian malware Backup positif palsu 1080
Mengatasi temuan 1082
Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan 1082
Memperbaiki bucket S3 yang berpotensi dikompromikan 1084
Rekomendasi berdasarkan kebutuhan akses bucket S3 tertentu 1086
Memperbaiki objek S3 yang berpotensi berbahaya 1087
Memperbaiki Snapshot EBS yang berpotensi dikompromikan 1087
Memperbaiki AMI EC2 yang berpotensi dikompromikan 1088
Memperbaiki Titik Pemulihan EC2 yang berpotensi terganggu 1089
Memperbaiki Titik Pemulihan S3 yang berpotensi dikompromikan 1090
Memperbaiki cluster ECS yang berpotensi dikompromikan 1091
Memperbaiki potensi terganggu AWS credentials 1092
Memperbaiki wadah mandiri yang berpotensi dikompromikan 1093
Memperbaiki temuan Perlindungan EKS 1095
Masalah konfigurasi potensial 1096
Memperbaiki pengguna Kubernetes yang berpotensi dikompromikan 1096
Memperbaiki pod Kubernetes yang berpotensi dikompromikan 1099
Memperbaiki gambar kontainer yang berpotensi dikompromikan 1100
Memperbaiki node Kubernetes yang berpotensi terganggu 1101
Memperbaiki temuan Pemantauan Runtime 1102
Memperbaiki gambar kontainer yang dikompromikan 1103
Memulihkan database yang berpotensi dikompromikan 1104
Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil 1105
Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal 1106

Memulihkan database yang berpotensi dikompromikan dengan aktivitas eksfiltrasi anomali ... 1107
Memulihkan database yang berpotensi dikompromikan dengan aktivitas destruktif anomali ... 1108
Memulihkan kredensi yang berpotensi dikompromikan ... 1110
Batasi akses jaringan ... 1110
Memperbaiki fungsi Lambda yang berpotensi dikompromikan ... 1111
Memantau penggunaan dan memperkirakan biaya ... 1112
Metrik CloudWatch Penggunaan Amazon ... 1112
Rincian Metrik ... 1112
Perlindungan Malware untuk S3 ... 1115
Memahami GuardDuty Penggunaan ... 1116
GuardDuty Pemrosesan Acara ... 1116
GuardDuty Biaya pemrosesan Log Aliran VPC untuk instans yang dipantau oleh GuardDuty Runtime Monitoring ... 1116
Memperkirakan biaya GuardDuty ... 1117
Penggunaan AWS Kalkulator Harga ... 1117
Pelanggan Hub Keamanan ... 1118
Nama fitur untuk paket perlindungan di API ... 1119
Ubah dari sumber data ke fitur ... 1119
GuardDuty Perubahan API ... 1119
Fitur dibandingkan dengan sumber data ... 1120
Memahami cara kerja API dengan fitur ... 1120
Memasukkan perubahan fitur dalam API ... 1121
Fitur yang dipetakan GuardDuty ... 1122
Keamanan ... 1125
Perlindungan data ... 1126
Enkripsi saat diam ... 1127
Enkripsi saat bergerak ... 1127
Memilih untuk tidak menggunakan data Anda untuk perbaikan layanan ... 1127
Logging dengan CloudTrail ... 1129
GuardDuty informasi di CloudTrail ... 1129
GuardDuty peristiwa pesawat kontrol di CloudTrail ... 1130
GuardDuty peristiwa data di CloudTrail ... 1130
Contoh: entri file GuardDuty log ... 1132
Identity and Access Management ... 1134

Audiens 1135
Mengautentikasi dengan identitas 1135
Mengelola akses menggunakan kebijakan 1137
Bagaimana Amazon GuardDuty bekerja dengan IAM 1138
Identity-based contoh kebijakan 1144
Menggunakan peran tertaut layanan 1154
AWS kebijakan yang dikelola 1164
Pemecahan masalah 1182
Validasi kepatuhan 1184
Ketahanan 1185
Keamanan infrastruktur 1185
Titik akhir VPC (AWS PrivateLink) 1186
Pertimbangan untuk titik akhir GuardDuty VPC 1186
Membuat titik akhir VPC antarmuka untuk GuardDuty 1186
Membuat kebijakan titik akhir VPC untuk GuardDuty 1187
Subnet bersama 1188
Integrasi dengan layanan AWS keamanan 1189
Integrasi dengan GuardDuty AWS Security Hub CSPM 1189
Integrasi GuardDuty dengan Amazon Detective 1189
AWS Security Hub CSPM integrasi 1189
Bagaimana Amazon GuardDuty mengirimkan temuan ke AWS Security Hub CSPM 1190
Melihat GuardDuty temuan di AWS Security Hub CSPM 1191
Mengaktifkan dan mengonfigurasi integrasi 1212
Menggunakan GuardDuty kontrol di Security Hub CSPM 1212
Menghentikan publikasi temuan ke Security Hub CSPM 1212
Integrasi Amazon Detective 1212
Mengaktifkan integrasi 1213
Berputar ke Detektif Amazon dari sebuah temuan GuardDuty 1213
Menggunakan integrasi dengan lingkungan GuardDuty multi-akun 1214
Menangguhkan atau menonaktifkan 1215
GuardDuty pengumuman 1217
Format pesan Amazon SNS 1223
GuardDuty kuota 1228
Support Instans Terkelola 1235
Pemecahan masalah 1236
Mengekspor temuan ke Amazon S3 - kesalahan akses 1236

Perlindungan Malware untuk masalah EC2 1237
Hilang diperlukan AWS Organizations izin manajemen saat mengaktifkan pemindaian GuardDuty-initiated malware 1237
Saya memulai pemindaian On-demand malware tetapi menghasilkan kesalahan izin yang diperlukan hilang. 1237
Saya menerima GetRole kesalahan `iam:` saat bekerja dengan Perlindungan Malware untuk EC2. 1237
Saya adalah akun GuardDuty administrator yang perlu mengaktifkan pemindaian GuardDuty-initiated malware tetapi tidak menggunakan AWS kebijakan terkelola: AmazonGuardDutyFullAccess untuk mengelola GuardDuty. 1238
Masalah Pemantauan Runtime 1238
Masalah cakupan runtime 1238
Memecahkan masalah kesalahan memori 1239
Saya AWS Step Functions alur kerja gagal secara tak terduga 1239
Masalah pemecahan masalah lainnya 1240
Wilayah dan titik akhir 1241
Region-specific ketersediaan fitur 1241
Tindakan dan parameter lama 1244
Riwayat dokumen 1246
Pembaruan lebih awal 1351
..... mccclii

Apa itu Amazon GuardDuty?

Amazon GuardDuty adalah layanan deteksi ancaman yang terus memantau, menganalisis, dan memproses sumber AWS data dan log di AWS lingkungan Anda. GuardDuty Menggunakan feed intelijen ancaman, seperti daftar alamat IP berbahaya dan domain, hash file, dan model machine learning (ML) untuk mengidentifikasi aktivitas mencurigakan dan berpotensi berbahaya di lingkungan Anda. AWS Daftar berikut memberikan ikhtisar skenario ancaman potensial yang GuardDuty dapat membantu Anda mendeteksi:

- Kredensi yang dikompromikan dan diekstraksi. AWS
- Eksfiltrasi dan penghancuran data yang dapat menyebabkan peristiwa ransomware. Pola peristiwa login yang tidak biasa dalam versi mesin yang didukung dari database Amazon Aurora dan Amazon RDS, yang menunjukkan perilaku anomali.
- Aktivitas cryptomining yang tidak sah di instans Amazon Elastic Compute Cloud (Amazon EC2) dan beban kerja container.
- Kehadiran malware di instans Amazon EC2 dan beban kerja kontainer, serta file yang baru diunggah di bucket Amazon Simple Storage Service (Amazon S3).
- Tingkat sistem operasi, jaringan, dan peristiwa file yang menunjukkan perilaku tidak sah pada kluster Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Service (Amazon ECS) - tugas, dan instans Amazon EC2 serta beban kerja AWS Fargate container.

Video berikut memberikan ikhtisar tentang bagaimana GuardDuty membantu Anda mendeteksi ancaman di AWS lingkungan Anda.

Apa itu Amazon GuardDuty

Daftar Isi

- Fitur GuardDuty
- Kepatuhan PCI DSS
- Harga di GuardDuty
- Mengakses GuardDuty

Fitur GuardDuty

Berikut adalah beberapa cara utama Amazon GuardDuty dapat membantu Anda memantau, mendeteksi, dan mengelola potensi ancaman di AWS lingkungan Anda.

Terus memantau sumber data tertentu dan log peristiwa

- Deteksi ancaman dasar — Ketika Anda mengaktifkan GuardDuty Akun AWS, GuardDuty secara otomatis mulai menelan sumber data dasar yang terkait dengan akun itu. Sumber data ini mencakup peristiwa AWS CloudTrail manajemen, log aliran VPC (dari instans Amazon EC2), dan log DNS. Anda tidak perlu mengaktifkan hal lain GuardDuty untuk mulai menganalisis dan

memproses sumber data ini untuk menghasilkan temuan keamanan terkait. Untuk informasi selengkapnya, lihat GuardDuty sumber data dasar.

- Extended Threat Detection — Kemampuan ini mendeteksi serangan multi-tahap yang menjangkau sumber data dasar, berbagai jenis sumber AWS daya, dan waktu, dalam file. Akun AWS Mungkin ada beberapa peristiwa di akun Anda yang, secara individual, tidak menampilkan diri sebagai ancaman yang jelas. Namun, ketika peristiwa ini diamati dalam urutan yang menunjukkan aktivitas yang mencurigakan, GuardDuty mengidentifikasinya sebagai urutan serangan. GuardDuty memberi tahu Anda dengan membuat jenis pencarian urutan serangan terkait untuk memberikan detail tentang urutan serangan yang diamati.

  Tanpa biaya tambahan yang terkait dengannya, Extended Threat Detection diaktifkan secara otomatis untuk masing-masing Akun AWS saat diaktifkan GuardDuty. Kemampuan ini tidak mengharuskan Anda untuk mengaktifkan rencana perlindungan yang berfokus pada kasus penggunaan apa pun. Namun, untuk meningkatkan luasnya keamanan ke sumber daya Amazon S3 Anda GuardDuty , rekomendasikan untuk mengaktifkan Perlindungan S3 di akun Anda. Ini akan membantu Extended Threat Detection untuk mengidentifikasi serangan multi-tahap yang berpotensi memengaruhi sumber daya Amazon S3 Anda.

  Untuk informasi selengkapnya tentang cara kerja kemampuan ini dan skenario ancaman apa yang dicakupnya, lihatGuardDuty Deteksi Ancaman yang Diperpanjang.
- Investigasi (Pratinjau) — GuardDuty Investigasi menyediakan analisis AI-powered keamanan GuardDuty temuan Anda. Anda dapat membuat investigasi untuk menganalisis temuan spesifik, akun, atau seluruh organisasi Anda, dan menerima ringkasan investigasi terstruktur dengan penilaian risiko, penilaian kepercayaan, klasifikasi MITRE ATT&CK®, dan langkah selanjutnya yang dapat ditindaklanjuti. Untuk informasi selengkapnya, lihat GuardDuty Investigasi (Pratinjau).
- Aturan Deteksi Kustom — Aturan Deteksi Kustom adalah pustaka aturan deteksi yang dikurasi di Amazon GuardDuty yang selaras dengan teknik aktor ancaman. Setiap aturan mendeteksi teknik tertentu dengan mengevaluasi bidang dalam peristiwa AWS CloudTrail manajemen atau dalam peristiwa Runtime Monitoring dari agen keamanan. GuardDuty Anda dapat menelusuri, mengaktifkan, dan mengelola aturan dari GuardDuty konsol atau melalui GuardDuty API. Untuk informasi selengkapnya, lihat Aturan Deteksi Kustom di GuardDuty.
- Use-case Rencana GuardDuty perlindungan terfokus — Untuk meningkatkan visibilitas deteksi ancaman ke dalam keamanan AWS lingkungan Anda, GuardDuty menawarkan paket perlindungan khusus yang dapat Anda pilih untuk diaktifkan. Paket perlindungan membantu Anda memantau log dan peristiwa dari AWS layanan lain. Sumber-sumber ini termasuk

log audit EKS, aktivitas login RDS, peristiwa data Amazon S3 CloudTrail di, volume EBS, Pemantauan Runtime di Amazon EKS, Amazon EC2, dan ECS-Fargate Amazon, log aktivitas jaringan Lambda, dan peristiwa AWS CloudTrail data dari Amazon Bedrock, Amazon Bedrock, dan Amazon AI untuk Perlindungan AI. AgentCore SageMaker GuardDutymengkonsolidasikan sumber log dan peristiwa ini di bawah istilah - Fitur. Anda dapat mengaktifkan satu atau lebih paket perlindungan khusus di dukungan Wilayah AWS kapan saja. GuardDuty akan mulai memantau, memproses, dan menganalisis aktivitas berdasarkan rencana perlindungan yang Anda aktifkan. Untuk informasi selengkapnya tentang setiap rencana perlindungan dan cara kerjanya, lihat dokumen rencana perlindungan yang sesuai.

Saat Anda mengaktifkan GuardDuty untuk pertama kalinya, GuardDuty secara otomatis mengaktifkan semua paket perlindungan kecuali Runtime Monitoring untuk akun Anda, dan menyertakannya dalam uji coba gratis 30 hari. Anda dapat menonaktifkan paket perlindungan apa pun kapan saja. Jika Anda adalah GuardDuty pelanggan yang sudah ada, paket perlindungan yang diluncurkan setelah Anda mengaktifkan tidak GuardDuty diaktifkan secara otomatis, dan Anda dapat memilih untuk mengaktifkannya. Untuk informasi tentang paket perlindungan mana yang diaktifkan secara default, lihatMenggunakan uji GuardDuty coba gratis 30 hari.

Rencana perlindungan	Deskripsi
Perlindungan AI	Mendeteksi ancaman terhadap beban kerja AI Anda yang menggunakan Amazon Bedrock, Amazon Bedrock, AgentCore dan Amazon SageMaker AI, seperti pemanggilan model anomali dan serangan biaya panen.
Perlindungan S3	Mengidentifikasi potensi risiko keamanan seperti eksfiltrasi data dan upaya penghancuran di bucket Amazon S3 Anda.
Perlindungan EKS	EKS Audit Log Monitoring menganalisis log audit Kubernete s dari klaster Amazon EKS Anda untuk aktivitas yang berpotensi mencurigakan dan berbahaya.
Pemantauan Runtime	Memantau dan menganalisis peristiwa tingkat sistem operasi di Amazon EKS, Amazon EC2, dan Amazon ECS Anda (AWS Fargate termasuk), untuk mendeteksi potensi ancaman runtime.

Rencana perlindungan	Deskripsi
Perlindungan Malware untuk EC2	Mendeteksi potensi keberadaan malware dengan memindai volume Amazon EBS yang terkait dengan instans Amazon EC2 Anda. Ada opsi untuk menggunakan fitur ini sesuai permintaan.
Perlindungan Malware untuk S3	Mendeteksi potensi keberadaan malware di objek yang baru diunggah dalam bucket Amazon S3 Anda. Ada opsi untuk menggunakan fitur ini sesuai permintaan.
Perlindungan Malware untuk AWS Backup	Mendeteksi potensi keberadaan malware dengan memindai sumber daya cadangan, termasuk EBS Snapshots, EC2 AMI, dan titik pemulihan Backup AWS . Ada opsi untuk menggunakan fitur ini sesuai permintaan.
Perlindungan RDS	Menganalisis dan membuat profil aktivitas login RDS Anda untuk potensi ancaman akses ke basis data Amazon Aurora dan Amazon RDS yang didukung.
Perlindungan Lambda	Memantau log aktivitas jaringan Lambda, dimulai dengan log aliran VPC, untuk mendeteksi ancaman terhadap fungsi Anda. AWS Lambda Contoh ancaman potensial ini termasuk cryptomining dan berkomunikasi dengan server jahat.

> **Aktifkan Perlindungan Malware untuk S3 secara mandiri**
>
> GuardDuty menawarkan fleksibilitas untuk menggunakan Perlindungan Malware untuk S3 secara independen, tanpa mengaktifkan layanan Amazon GuardDuty . Untuk informasi selengkapnya tentang memulai hanya dengan Perlindungan Malware untuk S3, lihatGuardDuty Perlindungan Malware untuk S3. Untuk menggunakan semua paket perlindungan lainnya, Anda harus mengaktifkan GuardDuty layanan.

Mengelola lingkungan multi-akun

Anda dapat mengelola AWS lingkungan beberapa akun dengan menggunakan metode undangan AWS Organizations (disarankan) atau lama. Untuk informasi selengkapnya, lihat Mengelola beberapa akun.

Menghasilkan temuan keamanan untuk ancaman yang terdeteksi

Ketika GuardDuty mendeteksi potensi ancaman keamanan yang terkait dengan AWS sumber daya Anda, itu mulai menghasilkan temuan keamanan yang memberikan informasi tentang sumber daya yang berpotensi dikompromikan. Setelah Anda mengaktifkan GuardDuty di akun Anda, buat Sampel temuan untuk melihat yang terkaitDetail temuan. Untuk daftar lengkap temuan keamanan, lihatGuardDuty menemukan jenis.

Dengan GuardDuty, Anda juga dapat menggunakan skrip penguji yang menghasilkan temuan GuardDuty keamanan khusus untuk memahami cara meninjau dan menanggapi GuardDuty temuan. Untuk informasi selengkapnya, lihat GuardDuty Temuan uji di akun khusus.

Menilai dan mengelola temuan keamanan

GuardDuty menggabungkan temuan keamanan Anda di seluruh akun dan menampilkan hasil di dasbor Ringkasan di GuardDuty konsol. Anda juga dapat mengambil temuan melalui AWS Security Hub CSPM API, AWS Command Line Interface, atau AWS SDK. Dengan pandangan holistik tentang status keamanan Anda saat ini, Anda dapat mengidentifikasi tren dan potensi masalah, dan mengambil langkah-langkah perbaikan yang diperlukan. Untuk informasi selengkapnya, lihat Mengelola GuardDuty temuan.

Integrasi dengan layanan AWS keamanan terkait

Untuk lebih membantu Anda menganalisis dan menyelidiki tren keamanan di AWS lingkungan Anda, pertimbangkan untuk menggunakan layanan AWS terkait keamanan berikut dalam kombinasi dengan. GuardDuty

- AWS Security Hub CSPM— Layanan ini memberi Anda pandangan komprehensif tentang keadaan keamanan AWS sumber daya Anda dan membantu Anda memeriksa AWS lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Hal ini dilakukan sebagian dengan mengkonsumsi, menggabungkan, mengatur, dan memprioritaskan temuan keamanan Anda dari berbagai layanan (AWS termasuk Amazon Macie) dan produk Jaringan Mitra (APN) yang didukung AWS . Security Hub CSPM membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi di lingkungan Anda AWS .

  Untuk informasi tentang penggunaan GuardDuty dan Security Hub CSPM bersama-sama, lihat. Integrasi dengan GuardDuty AWS Security Hub CSPM Untuk mempelajari CSPM Security Hub selengkapnya, lihat AWS Security Hub Panduan Pengguna.
- Detektif Amazon — Layanan ini membantu Anda menganalisis, menyelidiki, dan mengidentifikasi akar penyebab temuan keamanan atau aktivitas mencurigakan dengan cepat. Detective secara otomatis mengumpulkan data log dari sumber daya Anda. AWS Kemudian

menggunakan pembelajaran mesin, analisis statistik, dan teori grafik untuk menghasilkan visualisasi yang membantu Anda melakukan penyelidikan keamanan yang lebih cepat dan lebih efisien. Agregasi data Detective prebuilt, ringkasan, dan konteks membantu Anda menganalisis dan menentukan sifat dan tingkat potensi masalah keamanan.

Untuk informasi tentang penggunaan GuardDuty dan Detektif bersama-sama, lihat. Integrasi GuardDuty dengan Amazon Detective Untuk mempelajari lebih lanjut tentang Detektif, lihat Panduan Pengguna Detektif Amazon.

- Amazon EventBridge — Layanan ini membantu Anda menerima notifikasi dan menanggapi temuan GuardDuty keamanan dalam waktu dekat. GuardDuty menciptakan peristiwa ketika ada perubahan dalam temuan. Anda dapat memilih seberapa sering Anda ingin menerima notifikasi dari EventBridge. Untuk informasi selengkapnya, lihat Apa itu Amazon EventBridge di Panduan EventBridge Pengguna Amazon.

Kepatuhan PCI DSS

GuardDuty mendukung pemrosesan, penyimpanan, dan transmisi data kartu kredit oleh pedagang atau penyedia layanan, dan telah divalidasi sesuai dengan Standar Keamanan Data Industri Kartu Pembayaran (PCI) Data Security Standard (DSS). Untuk informasi selengkapnya tentang PCI DSS, termasuk cara meminta salinan PCI AWS Compliance Package, lihat PCI DSS Level 1.

Untuk informasi selengkapnya, lihat Pengujian pihak ketiga baru membandingkan Amazon GuardDuty dengan sistem deteksi intrusi jaringan di Blog Keamanan.AWS

Harga di GuardDuty

Bagian ini berfokus pada AWS Tingkat Gratis model yang GuardDuty digunakan untuk berbagai rencana perlindungan, dan bagaimana Anda dapat melihat perkiraan dan biaya penggunaan aktual. Jika Anda mencari detail harga yang terkait dengan semua paket perlindungan di seluruh Wilayah yang didukung, lihat GuardDutyharga.

AWS Tingkat Gratis

AWS Tingkat Gratis membantu Anda menjelajahi dan mencoba Layanan AWS secara gratis hingga batas yang ditentukan untuk setiap layanan. Ada tiga kategori — 12 bulan gratis, selalu gratis, dan uji coba gratis jangka pendek. Amazon GuardDuty termasuk dalam kategori uji coba gratis jangka pendek dan menawarkan uji coba gratis 30 hari. Ketika Anda terus menggunakan

GuardDuty setelah uji coba gratis ini berakhir, Anda mulai mengeluarkan biaya berdasarkan cara Anda menggunakan layanan ini.

[1] Pengecualian untuk uji GuardDuty coba gratis 30 hari

On-demand Pemindaian malware (di bawah Perlindungan Malware untuk EC2) dan Perlindungan Malware untuk S3 tidak termasuk dalam kategori uji coba gratis jangka pendek GuardDuty 30 hari. Perlindungan Malware untuk S3 mencakup Tingkat Gratis sedangkan pemindaian On-demand malware mengikuti model biaya bayar sesuai penggunaan. Tidak ada uji coba gratis 30 hari atau model biaya Tingkat Gratis dengan pemindaian On-demand malware.

Menggunakan uji GuardDuty coba gratis 30 hari

Saat menggunakan GuardDuty untuk pertama kalinya Wilayah AWS, Anda Akun AWS secara otomatis terdaftar dalam uji coba gratis 30 hari di Wilayah tersebut. Beberapa paket perlindungan juga akan diaktifkan secara otomatis dan termasuk dalam uji coba gratis 30 hari. Karena GuardDuty merupakan layanan regional, ketika Anda mengaktifkannya untuk pertama kalinya di Wilayah yang berbeda, akun Anda akan mendapatkan uji coba gratis 30 hari GuardDuty di Wilayah tersebut. Saat bekerja dengan beberapa akun dalam suatu GuardDuty organisasi, setiap akun mendapatkan uji coba gratis 30 hari sendiri.

Gunakan tabel berikut untuk meninjau paket perlindungan mana yang diaktifkan secara default GuardDuty, dan ketersediaan uji coba gratisnya.

Rencana perlindungan	Diaktifkan secara default dengan GuardDuty	Pisahkan ketersediaan uji coba gratis [2]	
Perlindungan EKS	Ya	Ya	
Perlindungan S3	Ya	Ya	
Pemantauan Runtime	Tidak	Ya	
Perlindungan Malware untuk EC2 – GuardDuty-initiated pemindaian malware	Ya	Ya	

Rencana perlindungan	Diaktifkan secara default dengan GuardDuty	Pisahkan ketersediaan uji coba gratis [2]	
Perlindungan Malware untuk EC2 – On-demand pemindaian malware GuardDuty	Tidak	Tidak [1]	
GuardDuty Perlindungan Malware untuk S3	Tidak	Tidak [1]	
Perlindungan RDS	Ya	Ya	
Perlindungan Lambda	Ya	Ya	
Perlindungan Malware untuk AWS Backup	Tidak	Tidak	

[2] Saat Anda mengaktifkan GuardDuty untuk pertama kalinya, paket perlindungan (kecuali Runtime Monitoring) secara otomatis diaktifkan dan disertakan dalam uji coba gratis 30 hari awal. Ketika GuardDuty akun yang ada memungkinkan rencana perlindungan baru setelah uji coba GuardDuty gratis awal mereka berakhir, maka paket perlindungan itu dilengkapi dengan uji coba gratis 30 hari sendiri. Untuk informasi selengkapnya tentang uji coba gratis untuk paket perlindungan, lihat dokumen yang terkait dengan setiap paket perlindungan.

Lihat perkiraan biaya penggunaan selama uji coba gratis — Selama uji coba gratis 30 hari GuardDuty dan kemungkinan rencana perlindungan, GuardDuty berikan perkiraan biaya penggunaan untuk akun Anda. Jika Anda adalah akun GuardDuty administrator yang didelegasikan, Anda dapat melihat total perkiraan biaya penggunaan dan rincian tingkat akun untuk semua akun anggota yang telah diaktifkan. GuardDuty Untuk informasi selengkapnya, lihat Memantau GuardDuty Penggunaan dan Memperkirakan Biaya.

Biaya penggunaan setelah uji coba gratis berakhir — Saat Anda terus menggunakan GuardDuty atau paket perlindungannya setelah uji coba gratis berakhir, Anda akan mulai mengeluarkan biaya penggunaan terkait. Untuk melihat tagihan Anda, navigasikan ke Cost Explorer di https://console.aws.amazon.com/costmanagement/konsol. Untuk informasi selengkapnya tentang penagihan AWS akun, lihat Panduan AWS Billing Pengguna.

Menggunakan Perlindungan Malware untuk S3 dengan Tingkat Gratis

Perlindungan Malware untuk S3 mencakup Tingkat Gratis yang terkait dengan Anda Akun AWS. Untuk informasi selengkapnya, lihat Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3.

Mengakses GuardDuty

Amazon GuardDuty tersedia di sebagian besar Wilayah AWS. Untuk daftar Wilayah yang saat GuardDuty ini tersedia, lihatWilayah dan titik akhir.

Anda dapat menggunakan GuardDuty salah satu cara berikut:

GuardDuty konsol

https://console.aws.amazon.com/guardduty/

Konsol adalah antarmuka berbasis browser untuk mengakses dan menggunakan. GuardDuty GuardDuty Konsol menyediakan akses ke GuardDuty akun, data, dan sumber daya Anda.

AWS Command Line Interface

Dengan AWS Command Line Interface (AWS CLI), Anda dapat mengeluarkan perintah di baris perintah sistem Anda untuk melakukan GuardDuty tugas dan AWS tugas. AWS CLI Perintah berguna jika Anda ingin membangun skrip yang melakukan tugas.

Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat Panduan AWS Command Line Interface Pengguna. Untuk melihat AWS CLI perintah yang tersedia GuardDuty, lihat Referensi AWS CLI Perintah.

GuardDuty HTTPS API

Anda dapat mengakses GuardDuty dan AWS secara terprogram menggunakan GuardDuty HTTPS API, yang memungkinkan Anda mengeluarkan permintaan HTTPS langsung ke layanan. Untuk informasi selengkapnya, lihat Referensi Amazon GuardDuty API.

AWS SDK

AWS menyediakan perangkat pengembangan perangkat lunak (SDK) yang terdiri dari pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman (Java, Python, Ruby, .NET, iOS, Android, dan lainnya). SDK menyediakan cara mudah untuk membuat akses terprogram ke.

GuardDuty Untuk informasi tentang AWS SDK, termasuk cara mengunduh dan menginstalnya, lihat Alat untuk Amazon Web Services.

Konsep dan istilah kunci di Amazon GuardDuty

Saat Anda memulai dengan Amazon GuardDuty, Anda bisa mendapatkan keuntungan dari mempelajari konsepnya dan istilah kunci terkait.

Akun

Akun Amazon Web Services (AWS) standar yang berisi AWS sumber daya Anda. Anda dapat masuk AWS dengan akun Anda dan mengaktifkan GuardDuty.

Anda juga dapat mengundang akun lain untuk mengaktifkan GuardDuty dan menjadi terkait dengan AWS akun Anda di GuardDuty. Jika undangan Anda diterima, akun Anda ditetapkan sebagai akun akun administrator, dan GuardDuty akun yang ditambahkan menjadi akun anggota Anda. Anda kemudian dapat melihat dan mengelola GuardDuty temuan akun tersebut atas nama mereka.

Pengguna akun administrator dapat mengonfigurasi GuardDuty serta melihat dan mengelola GuardDuty temuan untuk akun mereka sendiri dan semua akun anggota mereka. Untuk informasi tentang jumlah akun anggota yang dapat dikelola oleh akun administrator Anda, lihatGuardDuty kuota.

Pengguna akun anggota dapat mengonfigurasi GuardDuty serta melihat dan mengelola GuardDuty temuan di akun mereka (baik melalui konsol GuardDuty manajemen atau GuardDuty API). Pengguna akun anggota tidak dapat melihat atau mengelola temuan di akun anggota lain.

Tidak Akun AWS dapat menjadi akun GuardDuty administrator dan akun anggota secara bersamaan. An hanya Akun AWS dapat menerima satu undangan keanggotaan. Menerima undangan keanggotaan bersifat opsional.

Untuk informasi selengkapnya, lihat Mengelola banyak akun di Amazon GuardDuty.

Pola serangan

Urutan serangan adalah korelasi dari beberapa peristiwa yang, seperti yang diamati oleh GuardDuty, terjadi dalam urutan tertentu yang cocok dengan pola aktivitas yang mencurigakan. GuardDuty menggunakan Deteksi Ancaman yang Diperpanjang kemampuannya untuk mendeteksi serangan multi-tahap yang mencakup sumber data dasar, sumber AWS daya, dan garis waktu, di akun Anda.

Daftar berikut menjelaskan secara singkat istilah-istilah kunci yang terkait dengan urutan serangan:

- Indikator — Memberikan informasi mengapa urutan peristiwa sejalan dengan aktivitas yang mencurigakan potensial.
- Sinyal — Sinyal adalah aktivitas API yang GuardDuty diamati, atau GuardDuty temuan yang sudah terdeteksi di akun Anda. Dengan menghubungkan peristiwa yang diamati dalam urutan tertentu di akun Anda, GuardDuty mengidentifikasi urutan serangan.

  Ada peristiwa di akun Anda yang tidak menunjukkan potensi ancaman. GuardDuty menganggapnya sebagai sinyal lemah. Namun, ketika sinyal dan GuardDuty temuan lemah diamati dalam urutan tertentu yang, ketika berkorelasi, sejajar dengan aktivitas yang berpotensi mencurigakan, GuardDuty menghasilkan temuan urutan serangan.
- Endpoints — Informasi tentang titik akhir jaringan yang berpotensi digunakan oleh aktor ancaman dalam urutan serangan.

Detektor

Amazon GuardDuty adalah layanan regional. Saat Anda mengaktifkan GuardDuty secara spesifik Wilayah AWS, Anda Akun AWS akan dikaitkan dengan ID detektor. ID alfanumerik 32 karakter ini unik untuk akun Anda di Wilayah tersebut. Misalnya, ketika Anda mengaktifkan GuardDuty akun yang sama di Wilayah yang berbeda, akun Anda akan dikaitkan dengan ID detektor yang berbeda. Format detectorID adalah. `12abc34d567e8fa901bc2d34e56789f0`

Semua GuardDuty temuan, akun, dan tindakan tentang mengelola temuan dan GuardDuty layanan menggunakan ID detektor untuk menjalankan operasi API.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

> **Note**
>
> Di lingkungan multi-akun, semua temuan untuk akun anggota digulung ke detektor akun administrator.

Beberapa GuardDuty fungsi dikonfigurasi melalui detektor, seperti mengonfigurasi frekuensi pemberitahuan CloudWatch Acara, dan mengaktifkan atau menonaktifkan rencana perlindungan opsional untuk diproses. GuardDuty

Menggunakan Perlindungan Malware untuk S3 di dalam GuardDuty

Saat Anda mengaktifkan Perlindungan Malware untuk S3 di akun yang GuardDuty diaktifkan, Perlindungan Malware untuk tindakan S3 seperti mengaktifkan, mengedit, dan menonaktifkan sumber daya yang dilindungi tidak terkait dengan ID detektor.

Jika Anda tidak mengaktifkan GuardDuty dan memilih opsi deteksi ancaman Perlindungan Malware untuk S3, tidak ada ID detektor yang dibuat untuk akun Anda.

Sumber data dasar

Asal atau lokasi satu set data. Untuk mendeteksi aktivitas yang tidak sah atau tidak terduga di AWS lingkungan Anda. GuardDuty menganalisis dan memproses data dari log AWS CloudTrail peristiwa, peristiwa AWS CloudTrail manajemen, peristiwa AWS CloudTrail data untuk S3, log aliran VPC, log DNS, lihat. GuardDuty sumber data dasar

Fitur

Objek fitur yang dikonfigurasi untuk paket GuardDuty perlindungan Anda membantu mendeteksi aktivitas yang tidak sah atau tidak terduga di AWS lingkungan Anda. Setiap rencana GuardDuty perlindungan mengkonfigurasi objek fitur yang sesuai untuk menganalisis dan memproses data. Beberapa objek fitur termasuk log audit EKS, pemantauan aktivitas login RDS, log aktivitas jaringan Lambda, dan volume EBS. Untuk informasi selengkapnya, lihat Nama fitur untuk paket perlindungan di GuardDuty API.

Menemukan

Masalah keamanan potensial ditemukan oleh GuardDuty. Untuk informasi selengkapnya, lihat Memahami dan menghasilkan GuardDuty temuan Amazon.

Temuan ditampilkan di GuardDuty konsol dan berisi deskripsi rinci tentang masalah keamanan. Anda juga dapat mengambil temuan yang dihasilkan dengan memanggil operasi GetFindingsdan ListFindingsAPI.

Anda juga dapat melihat GuardDuty temuan Anda melalui CloudWatch acara Amazon. GuardDuty mengirimkan temuan ke Amazon CloudWatch melalui protokol HTTPS. Untuk informasi selengkapnya, lihat Memproses GuardDuty temuan dengan Amazon EventBridge.

Peran IAM

Ini adalah peran IAM dengan izin yang diperlukan untuk memindai objek S3. Saat menandai objek yang dipindai diaktifkan, PassRole izin IAM membantu GuardDuty menambahkan tag ke objek yang dipindai.

Sumber daya paket Perlindungan Malware

Setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk bucket, GuardDuty buat sumber daya paket Perlindungan Malware. Sumber daya ini dikaitkan dengan ID paket Perlindungan Malware, pengenal unik untuk bucket Anda yang dilindungi. Gunakan sumber daya paket Perlindungan Malware untuk melakukan operasi API pada sumber daya yang dilindungi.

Ember yang dilindungi (sumber daya terlindungi)

Bucket Amazon S3 dianggap dilindungi saat Anda mengaktifkan Perlindungan Malware untuk S3 untuk bucket ini dan status perlindungannya berubah menjadi Aktif.

GuardDuty hanya mendukung bucket S3 sebagai sumber daya yang dilindungi.

Status perlindungan

Status yang terkait dengan sumber daya paket Perlindungan Malware Anda. Setelah mengaktifkan Perlindungan Malware untuk S3 untuk bucket, status ini menunjukkan apakah bucket sudah diatur dengan benar atau tidak.

Awalan objek S3

Di bucket Amazon Simple Storage Service (Amazon S3), Anda dapat menggunakan awalan untuk mengatur penyimpanan Anda. Awalan adalah pengelompokan logis objek dalam ember S3. Untuk informasi selengkapnya, lihat Mengatur dan mencantumkan objek di Panduan Pengguna Amazon S3.

Opsi pemindaian

Saat Perlindungan GuardDuty Malware untuk EC2 diaktifkan, Anda dapat menentukan instans Amazon EC2 dan volume Amazon Elastic Block Store (EBS) mana yang akan dipindai atau dilewati. Fitur ini memungkinkan Anda menambahkan tag yang ada yang terkait dengan instans EC2 dan volume EBS Anda ke daftar tag inklusi atau daftar tag pengecualian. Sumber daya yang terkait dengan tag yang Anda tambahkan ke daftar tag inklusi, dipindai untuk malware, dan yang ditambahkan ke daftar tag pengecualian tidak dipindai. Untuk informasi selengkapnya, lihat Opsi pindai dengan tag yang ditentukan pengguna.

Retensi snapshot

Ketika Perlindungan GuardDuty Malware untuk EC2 diaktifkan, ini menyediakan opsi untuk menyimpan snapshot volume EBS Anda di akun Anda. AWS GuardDuty menghasilkan replika volume EBS berdasarkan snapshot volume EBS Anda. Anda dapat menyimpan snapshot volume EBS Anda hanya jika Perlindungan Malware untuk pemindaian EC2 mendeteksi malware

dalam volume replika EBS. Jika tidak ada malware yang terdeteksi dalam volume replika EBS, GuardDuty secara otomatis menghapus snapshot volume EBS Anda, terlepas dari pengaturan retensi snapshot. Untuk informasi selengkapnya, lihat Retensi snapshot.

Aturan penindasan

Aturan penekanan memungkinkan Anda membuat kombinasi atribut yang sangat spesifik untuk menekan temuan. Misalnya, Anda dapat menentukan aturan melalui GuardDuty filter untuk mengarsipkan otomatis hanya `Recon:EC2/Portscan` dari instance tersebut di VPC tertentu, menjalankan AMI tertentu, atau dengan tag EC2 tertentu. Aturan ini akan mengakibatkan temuan pemindaian port diarsipkan secara otomatis dari instans yang memenuhi kriteria. Namun, masih memungkinkan peringatan jika GuardDuty mendeteksi instans yang melakukan aktivitas berbahaya lainnya, seperti penambangan mata uang kripto.

Aturan penindasan yang ditentukan dalam akun GuardDuty administrator berlaku untuk akun GuardDuty anggota. GuardDuty akun anggota tidak dapat mengubah aturan penindasan.

Dengan aturan penindasan, GuardDuty masih menghasilkan semua temuan. Aturan penekanan memberikan penekanan pada temuan sekaligus mempertahankan riwayat yang lengkap dan tidak berubah dari semua aktivitas.

Biasanya aturan penindasan digunakan untuk menyembunyikan temuan yang telah Anda tentukan sebagai positif palsu untuk lingkungan Anda, dan mengurangi kebisingan dari temuan bernilai rendah sehingga Anda dapat fokus pada ancaman yang lebih besar. Untuk informasi selengkapnya, lihat Aturan penindasan di GuardDuty.

Daftar IP tepercaya

Daftar alamat IP tepercaya untuk komunikasi yang sangat aman dengan AWS lingkungan Anda. GuardDuty tidak menghasilkan temuan berdasarkan daftar IP tepercaya. Untuk informasi selengkapnya, lihat Menyesuaikan deteksi ancaman dengan daftar entitas dan daftar alamat IP.

Daftar IP ancaman

Daftar alamat IP berbahaya yang diketahui. Selain menghasilkan temuan karena aktivitas yang berpotensi mencurigakan, GuardDuty juga menghasilkan temuan berdasarkan daftar ancaman ini. Lihat informasi yang lebih lengkap di Menyesuaikan deteksi ancaman dengan daftar entitas dan daftar alamat IP.

Memulai dengan GuardDuty

Tutorial ini memberikan pengantar langsung untuk. GuardDuty Persyaratan minimum untuk mengaktifkan GuardDuty sebagai akun mandiri atau sebagai GuardDuty administrator AWS Organizations tercakup dalam Langkah 1. Langkah 2 hingga 5 mencakup menggunakan fitur tambahan yang direkomendasikan oleh GuardDuty untuk mendapatkan hasil maksimal dari temuan Anda.

Topik

- Sebelum Anda mulai
- Langkah 1: Aktifkan Amazon GuardDuty
- Langkah 2: Menghasilkan temuan sampel dan menjelajahi operasi dasar
- Langkah 3: Konfigurasikan GuardDuty temuan ekspor ke bucket Amazon S3
- Langkah 4: Siapkan peringatan GuardDuty pencarian melalui SNS
- Langkah selanjutnya

Sebelum Anda mulai

GuardDuty adalah layanan deteksi ancaman yang memantau Sumber data dasar seperti peristiwa AWS CloudTrail manajemen, Amazon VPC Flow Logs, dan log kueri Amazon Route 53 Resolver DNS. GuardDutyjuga menganalisis fitur yang terkait dengan jenis perlindungannya hanya jika Anda mengaktifkannya secara terpisah. Fitur termasuk log audit Kubernetes, aktivitas login RDS, peristiwa AWS CloudTrail data untuk Amazon S3, volume Amazon EBS, Pemantauan Runtime, dan log aktivitas jaringan Lambda. Menggunakan sumber dan fitur data ini (jika diaktifkan), GuardDuty menghasilkan temuan keamanan untuk akun Anda.

Setelah Anda mengaktifkan GuardDuty, itu mulai memantau akun Anda untuk potensi ancaman berdasarkan aktivitas di sumber data dasar. Secara default, Deteksi Ancaman yang Diperpanjang diaktifkan untuk semua Akun AWS yang telah diaktifkan GuardDuty. Kemampuan ini mendeteksi urutan serangan multi-tahap yang mencakup beberapa sumber data dasar, sumber AWS daya, dan waktu, di akun Anda. Untuk mendeteksi potensi ancaman terhadap AWS sumber daya tertentu, Anda dapat memilih untuk mengaktifkan paket perlindungan yang berfokus pada kasus penggunaan yang GuardDuty menawarkan. Untuk informasi selengkapnya, lihat Fitur GuardDuty.

Anda tidak perlu mengaktifkan salah satu sumber data dasar secara eksplisit. Saat mengaktifkan Perlindungan S3, Anda tidak perlu mengaktifkan pencatatan peristiwa data Amazon S3 secara

eksplisit. Demikian pula, saat Anda mengaktifkan Perlindungan EKS, Anda tidak perlu mengaktifkan log audit Amazon EKS secara eksplisit. Amazon GuardDuty menarik aliran data independen langsung dari layanan ini.

Untuk GuardDuty akun baru, beberapa jenis perlindungan yang tersedia yang didukung dalam akun Wilayah AWS diaktifkan dan disertakan dalam periode uji coba gratis 30 hari secara default. Anda dapat memilih keluar dari salah satu atau semua dari mereka. Jika sudah ada Akun AWS dengan GuardDuty diaktifkan, Anda dapat memilih untuk mengaktifkan salah satu atau semua paket perlindungan yang tersedia di Wilayah Anda. Untuk ikhtisar rencana perlindungan dan rencana perlindungan mana yang akan diaktifkan secara default, lihatHarga di GuardDuty.

Saat mengaktifkan GuardDuty, pertimbangkan item berikut:

- GuardDuty adalah layanan Regional, artinya prosedur konfigurasi apa pun yang Anda ikuti di halaman ini harus diulang di setiap Wilayah yang ingin Anda pantau GuardDuty.

  Kami sangat menyarankan agar Anda mengaktifkan GuardDuty di semua AWS Wilayah yang didukung. Hal ini memungkinkan GuardDuty untuk menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa bahkan di Wilayah yang tidak Anda gunakan secara aktif. Ini juga memungkinkan GuardDuty untuk memantau AWS CloudTrail acara untuk AWS layanan global seperti IAM. Jika tidak GuardDuty diaktifkan di semua Wilayah yang didukung, kemampuannya untuk mendeteksi aktivitas yang melibatkan layanan global berkurang. Untuk daftar lengkap Wilayah yang GuardDuty tersedia, lihatWilayah dan titik akhir.
- Setiap pengguna dengan hak administrator di AWS akun dapat mengaktifkan GuardDuty, namun, mengikuti praktik keamanan terbaik dengan hak istimewa terkecil, disarankan agar Anda membuat peran, pengguna, atau grup IAM untuk dikelola secara khusus. GuardDuty Untuk informasi tentang izin yang diperlukan untuk mengaktifkan GuardDuty lihatIzin diperlukan untuk mengaktifkan GuardDuty.
- Saat Anda mengaktifkan GuardDuty untuk pertama kalinya di salah satu Wilayah AWS, secara default, ini juga memungkinkan semua jenis perlindungan yang tersedia yang didukung di Wilayah tersebut, termasuk Perlindungan Malware untuk EC2. GuardDuty membuat peran terkait layanan untuk akun Anda yang dipanggil. `AWSServiceRoleForAmazonGuardDuty` Peran ini mencakup izin dan kebijakan kepercayaan yang memungkinkan GuardDuty untuk mengkonsumsi dan menganalisis peristiwa secara langsung dari GuardDuty sumber data dasar untuk menghasilkan temuan keamanan. Perlindungan Malware untuk EC2 menciptakan peran terkait layanan lain untuk akun Anda yang dipanggil. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Peran ini mencakup izin dan kebijakan kepercayaan yang memungkinkan Perlindungan Malware untuk EC2 melakukan pemindaian tanpa agen untuk mendeteksi malware di akun Anda.

GuardDuty Ini memungkinkan GuardDuty untuk membuat snapshot volume EBS di akun Anda, dan berbagi snapshot itu dengan akun layanan. GuardDuty Untuk informasi selengkapnya, lihat Service-linked izin peran untuk GuardDuty. Untuk informasi selengkapnya tentang peran terkait layanan, lihat Menggunakan peran terkait layanan.

- Saat Anda mengaktifkan GuardDuty untuk pertama kalinya di Wilayah mana pun, AWS akun Anda secara otomatis terdaftar dalam uji coba GuardDuty gratis 30 hari untuk Wilayah tersebut.

Video berikut menjelaskan bagaimana akun administrator dapat memulai GuardDuty dan mengaktifkannya di beberapa akun anggota.

Memulai: Mengaktifkan Amazon GuardDuty untuk lingkungan mandiri atau multi-akun

Langkah 1: Aktifkan Amazon GuardDuty

Langkah pertama yang harus digunakan GuardDuty adalah mengaktifkannya di akun Anda. Setelah diaktifkan, GuardDuty akan segera mulai memantau ancaman keamanan di Wilayah saat ini.

Jika Anda ingin mengelola GuardDuty temuan untuk akun lain dalam organisasi Anda sebagai GuardDuty administrator, Anda harus menambahkan akun anggota dan GuardDuty mengaktifkannya juga.

> **Note**
>
> Jika Anda ingin mengaktifkan Perlindungan GuardDuty Malware untuk S3 tanpa mengaktifkan GuardDuty, maka untuk langkah-langkahnya, lihat. GuardDuty Perlindungan Malware untuk S3

Standalone account environment

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/
2. Pilih opsi Amazon GuardDuty - Semua fitur.
3. Pilih Mulai.
4. Pada GuardDuty halaman Selamat Datang di, lihat persyaratan layanan. Pilih Aktifkan GuardDuty.

Multi-account environment

> **Important**
>
> Sebagai prasyarat untuk proses ini, Anda harus berada di organisasi yang sama dengan semua akun yang ingin Anda kelola, dan memiliki akses ke akun AWS Organizations manajemen untuk mendelegasikan administrator di dalam organisasi Anda. GuardDuty Izin tambahan mungkin diperlukan untuk mendelegasikan administrator, untuk info selengkapnya, lihat Izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty.

Untuk menunjuk akun administrator yang didelegasikan GuardDuty

1. Buka AWS Organizations konsol di https://console.aws.amazon.com/organizations/, menggunakan akun manajemen.
2. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Apakah GuardDuty sudah diaktifkan di akun Anda?

   - Jika belum GuardDuty diaktifkan, Anda dapat memilih Memulai dan kemudian menunjuk administrator yang GuardDuty didelegasikan pada halaman Selamat Datang GuardDuty di.

- Jika GuardDuty diaktifkan, Anda dapat menunjuk administrator yang GuardDuty didelegasikan pada halaman Pengaturan.

3. Masukkan ID AWS akun dua belas digit dari akun yang ingin Anda tetapkan sebagai administrator yang GuardDuty didelegasikan untuk organisasi dan pilih Delegasi.

> **Note**
>
> Jika belum GuardDuty diaktifkan, menunjuk administrator yang didelegasikan akan mengaktifkan GuardDuty akun tersebut di Wilayah Anda saat ini.

Untuk menambahkan akun anggota

Prosedur ini mencakup penambahan akun anggota ke akun administrator yang GuardDuty didelegasikan melalui AWS Organizations. Ada juga opsi untuk menambahkan anggota melalui undangan. Untuk mempelajari lebih lanjut tentang kedua metode untuk mengasosiasikan anggota GuardDuty, lihatMengelola banyak akun di Amazon GuardDuty.

1. Masuk ke akun administrator yang didelegasikan
2. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
3. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.

   Tabel akun menampilkan semua akun dalam organisasi.
4. Pilih akun yang ingin Anda tambahkan sebagai anggota dengan mencentang kotak di samping ID akun. Kemudian dari menu Tindakan, pilih Tambah anggota.

> **Tip**
>
> Anda dapat mengotomatiskan penambahan akun baru sebagai anggota dengan mengaktifkan Auto-enablefitur; namun, ini hanya berlaku untuk akun yang bergabung dengan organisasi Anda setelah fitur diaktifkan.

Langkah 2: Menghasilkan temuan sampel dan menjelajahi operasi dasar

Ketika GuardDuty menemukan masalah keamanan, itu menghasilkan temuan. GuardDuty Temuan adalah kumpulan data yang berisi detail yang berkaitan dengan masalah keamanan unik itu. Detail temuan dapat digunakan untuk membantu Anda menyelidiki masalah tersebut.

GuardDuty mendukung menghasilkan temuan sampel dengan nilai placeholder, yang dapat digunakan untuk menguji GuardDuty fungsionalitas dan membiasakan diri dengan temuan sebelum perlu menanggapi masalah keamanan nyata yang ditemukan oleh. GuardDuty Ikuti panduan di bawah ini untuk menghasilkan temuan sampel untuk setiap jenis temuan yang tersedia di GuardDuty, untuk cara tambahan untuk menghasilkan temuan sampel, termasuk menghasilkan peristiwa keamanan simulasi dalam akun Anda, lihatSampel temuan.

Untuk membuat dan mengeksplorasi temuan sampel

1. Pada panel navigasi, silakan pilih Pengaturan.
2. Di halaman Pengaturan, di bawah Sampel temuan, pilih Buat sampel temuan.
3. Di panel navigasi, pilih Ringkasan untuk melihat wawasan tentang temuan yang dihasilkan di lingkungan Anda AWS . Untuk informasi selengkapnya tentang komponen dasbor Ringkasan, lihatDasbor ringkasan di Amazon GuardDuty.
4. Di panel navigasi, pilih Temuan. Temuan sampel ditampilkan pada halaman Temuan saat ini dengan prefiks [SAMPEL].
5. Pilih temuan dari daftar untuk menampilkan detail temuan.

    - Anda dapat meninjau bidang informasi yang berbeda yang tersedia di panel detail temuan. Berbagai jenis temuan dapat memiliki bidang yang berbeda. Untuk informasi selengkapnya tentang bidang yang tersedia di semua jenis pencarian, lihatDetail temuan. Dari panel detail, Anda dapat mengambil tindakan berikut:

        - Pilih ID temuan di bagian atas panel untuk membuka detail JSON lengkap untuk temuan. File JSON yang lengkap juga dapat diunduh dari panel ini. JSON berisi beberapa informasi tambahan yang tidak disertakan dalam tampilan konsol dan merupakan format yang dapat digunakan oleh alat dan layanan lainnya.
        - Lihat bagian Sumber daya yang terpengaruh. Dalam temuan nyata, informasi di sini akan membantu Anda mengidentifikasi sumber daya di akun Anda yang harus diselidiki dan

akan menyertakan tautan ke sumber daya yang sesuai Konsol Manajemen AWS untuk ditindaklanjuti.

- Pilih ikon kaca pembesar dengan + atau - untuk membuat filter inklusif atau eksklusif untuk detail tersebut. Untuk informasi selengkapnya tentang menemukan filter, lihatPenyaringan temuan di GuardDuty.

6. Arsipkan semua temuan sampel Anda

   a. Pilih semua temuan dengan memilih kotak centang di bagian atas daftar.

   b. Hapus pilihan temuan apa pun yang ingin Anda simpan.

   c. Pilih menu Tindakan, lalu pilih Arsip untuk menyembunyikan temuan sampel.

> **Note**
>
> Untuk melihat temuan yang diarsipkan, pilih Saat ini, lalu pilih Diarsipkan untuk beralih tampilan temuan.

Langkah 3: Konfigurasikan GuardDuty temuan ekspor ke bucket Amazon S3

GuardDuty merekomendasikan konfigurasi pengaturan untuk mengekspor temuan karena memungkinkan Anda untuk mengekspor temuan Anda ke bucket S3 untuk penyimpanan tidak terbatas di luar periode retensi 90 hari. GuardDuty Ini memungkinkan Anda untuk menyimpan catatan temuan atau melacak masalah dalam AWS lingkungan Anda dari waktu ke waktu. GuardDuty mengenkripsi data temuan di bucket S3 Anda dengan menggunakan AWS Key Management Service ().AWS KMS key Untuk mengkonfigurasi pengaturan, Anda harus memberikan GuardDuty izin kunci KMS. Untuk langkah-langkah lebih rinci, lihatMengekspor temuan yang dihasilkan ke Amazon S3.

Untuk mengekspor GuardDuty temuan ke ember Amazon S3

1. Lampirkan kebijakan ke kunci KMS

   a. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Key Management Service (AWS KMS) di https://console.aws.amazon.com/kms.

   b. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.

   c. Di panel navigasi, pilih Kunci yang dikelola pelanggan.

d. Pilih kunci KMS yang ada, atau lakukan langkah-langkah untuk Membuat kunci KMS enkripsi simetris di Panduan PengembangAWS Key Management Service .

   Wilayah kunci KMS dan bucket Amazon S3 Anda harus sama.

   Salin kunci ARN ke notepad untuk digunakan di langkah selanjutnya.

e. Di bagian Kebijakan kunci pada kunci KMS Anda, pilih Edit. Jika Beralih ke tampilan kebijakan ditampilkan, pilih untuk menampilkan Kebijakan kunci, lalu pilih Edit.

f. Salin blok kebijakan berikut ke kebijakan kunci KMS Anda:

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

   Edit kebijakan dengan mengganti nilai berikut yang diformat *red*dalam contoh kebijakan:

   1. Ganti *KMS key ARN* dengan Nama Sumber Daya Amazon (ARN) dari kunci KMS. Untuk menemukan kunci ARN, lihat Menemukan ID kunci dan ARN di Panduan Pengembang.AWS Key Management Service
   2. Ganti *123456789012* dengan Akun AWS ID yang memiliki GuardDuty akun yang mengekspor temuan.
   3. Ganti *Region2* dengan Wilayah AWS tempat GuardDuty temuan dihasilkan.
   4. Ganti *SourceDetectorID* dengan GuardDuty akun di Wilayah tertentu tempat temuan dihasilkan. `detectorID`

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

2. Lampirkan kebijakan ke bucket Amazon S3

   Jika Anda belum memiliki bucket Amazon S3 tempat Anda ingin mengekspor temuan ini, lihat Membuat bucket di Panduan Pengguna Amazon S3.

   a. Lakukan langkah-langkah di bawah Untuk membuat atau mengedit kebijakan bucket di Panduan Pengguna Amazon S3, hingga halaman Edit kebijakan bucket muncul.

   b. Kebijakan contoh menunjukkan cara memberikan GuardDuty izin untuk mengekspor temuan ke bucket Amazon S3 Anda. Jika Anda mengubah jalur setelah mengonfigurasi temuan ekspor, Anda harus mengubah kebijakan untuk memberikan izin ke lokasi baru.

      Salin contoh kebijakan berikut dan tempelkan ke editor kebijakan Bucket.

      Jika Anda menambahkan pernyataan kebijakan sebelum pernyataan akhir, tambahkan koma sebelum menambahkan pernyataan ini. Pastikan bahwa sintaks JSON dari kebijakan kunci KMS Anda valid.

      Kebijakan contoh bucket S3

      JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Allow GetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
```

```
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "Allow PutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "Deny unencrypted object uploads",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "Deny incorrect encryption header",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
```

```
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
                "StringNotEquals": {
                "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:us-east-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

c. Edit kebijakan dengan mengganti nilai berikut yang diformat *red*dalam contoh kebijakan:

1. Ganti *Amazon S3 bucket ARN* dengan Nama Sumber Daya Amazon (ARN) dari bucket Amazon S3. Anda dapat menemukan Bucket ARN di halaman kebijakan Edit bucket di konsol. https://console.aws.amazon.com/s3/
2. Ganti *123456789012* dengan Akun AWS ID yang memiliki GuardDuty akun yang mengekspor temuan.
3. Ganti *Region2* dengan Wilayah AWS tempat GuardDuty temuan dihasilkan.
4. Ganti *SourceDetectorID* dengan GuardDuty akun di Wilayah tertentu tempat temuan dihasilkan. `detectorID`

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

5. Ganti *`[optional prefix]`* bagian dari nilai *`S3 bucket ARN/[optional prefix]`* placeholder dengan lokasi folder opsional yang ingin Anda ekspor temuannya. Untuk informasi selengkapnya tentang penggunaan awalan, lihat Mengatur objek menggunakan awalan di Panduan Pengguna Amazon S3.

   Bila Anda menyediakan lokasi folder opsional yang belum ada, GuardDuty akan membuat lokasi tersebut hanya jika akun yang terkait dengan bucket S3 sama dengan akun yang mengekspor temuan. Saat Anda mengekspor temuan ke bucket S3 milik akun lain, lokasi folder harus sudah ada.

6. Ganti *`KMS key ARN`* dengan Nama Sumber Daya Amazon (ARN) dari kunci KMS yang terkait dengan enkripsi temuan yang diekspor ke bucket S3. Untuk menemukan kunci ARN, lihat Menemukan ID kunci dan ARN di Panduan Pengembang.AWS Key Management Service

3. Langkah-langkah di GuardDuty konsol

   a. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   b. Pada panel navigasi, silakan pilih Pengaturan.

   c. Pada halaman Pengaturan, di bawah opsi ekspor temuan, untuk bucket S3, pilih Konfigurasi sekarang (atau Edit, sesuai kebutuhan).

   d. Untuk S3 bucket ARN, masukkan **`bucket ARN`** yang ingin Anda kirimi temuannya. Untuk melihat ARN bucket, lihat Melihat properti untuk bucket S3 di Panduan Pengguna Amazon S3.

   e. Untuk ARN kunci KMS, masukkan file. **`key ARN`** Untuk menemukan kunci ARN, lihat Temukan ID kunci dan kunci ARN di Panduan Pengembang.AWS Key Management Service

   f. Pilih Simpan.

Langkah 4: Siapkan peringatan GuardDuty pencarian melalui SNS

GuardDuty terintegrasi dengan Amazon EventBridge, yang dapat digunakan untuk mengirim data temuan ke aplikasi dan layanan lain untuk diproses. Dengan EventBridge Anda dapat menggunakan GuardDuty temuan untuk memulai respons otomatis terhadap temuan Anda dengan menghubungkan

peristiwa pencarian ke target seperti AWS Lambda fungsi, otomatisasi Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS), dan lainnya.

Dalam contoh ini Anda akan membuat topik SNS untuk menjadi target EventBridge aturan, lalu Anda akan menggunakan EventBridge untuk membuat aturan yang menangkap data temuan dari. GuardDuty Aturan yang dihasilkan akan meneruskan detail temuan ke alamat email. Untuk mempelajari bagaimana Anda dapat mengirim temuan ke Slack atau Amazon Chime, dan juga memodifikasi jenis peringatan temuan yang dikirim, lihat. Siapkan topik dan titik akhir Amazon SNS

Untuk membuat topik SNS untuk peringatan temuan Anda

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Di panel navigasi, pilih Pengguna.
3. Pilih Buat Topik.
4. Untuk Jenis, pilih Standar.
5. Untuk Nama, masukkan **`GuardDuty`**.
6. Pilih Buat Topik. Detail topik untuk topik baru Anda akan terbuka.
7. Di bagian Subscriptions (Berlangganan), pilih Create subscription (Buat langganan).
8. Untuk Protokol, pilih Email.
9. Untuk Endpoint, masukkan alamat email untuk mengirim notifikasi.
10. Pilih Buat langganan.

    Setelah Anda membuat langganan, Anda harus mengonfirmasi langganan melalui email.
11. Untuk memeriksa pesan langganan, buka kotak masuk email Anda, dan di pesan berlangganan, pilih Konfirmasi langganan.

> **Note**
>
> Untuk memeriksa status konfirmasi email, buka konsol SNS dan pilih Langganan.

Untuk membuat EventBridge aturan untuk menangkap GuardDuty temuan dan memformatnya

1. Buka EventBridge konsol di https://console.aws.amazon.com/events/.
2. Di panel navigasi, di bawah Bus, pilih Aturan.
3. Pilih Buat aturan.

4. Masukkan nama dan deskripsi untuk aturan.

   Aturan tidak boleh memiliki nama yang sama dengan aturan lain di Wilayah yang sama dan di bus kejadian yang sama.

5. Untuk bus Acara, pastikan bahwa default dipilih dan Aktifkan aturan pada bus acara yang dipilih diaktifkan.
6. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
7. Pilih Selanjutnya.
8. Pada halaman pola acara Build, untuk sumber acara, pilih AWS acara atau acara EventBridge mitra.
9. Di bagian pola Event, untuk metode Creation, pilih Use pattern form.
10. Untuk Sumber peristiwa, pilih Layanan AWS .
11. Untuk Layanan AWS , pilih GuardDuty.
12. Untuk jenis Event, pilih GuardDutyFinding.
13. Pilih Berikutnya.
14. Untuk Tipe Target, pilih Layanan AWS .
15. Untuk Pilih target, pilih Topik SNS. Untuk lokasi Target, pilih Target di akun ini. Untuk Topik, pilih nama topik SNS yang Anda buat sebelumnya.
16. Perluas Pengaturan tambahan. Untuk Konfigurasi input target, pilih Trafo input.

    Menambahkan transformator input memformat data pencarian JSON yang dikirim dari GuardDuty ke dalam pesan yang dapat dibaca manusia.

17. Pilih Konfigurasikan transformator input.
18. Di bagian Transformator input target, untuk jalur Input, tempel kode berikut:

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_Description": "$.detail.description"
}
```

19. Untuk memformat email, untuk Template, tempel kode berikut. Saat EventBridge mengirimkan setiap temuan, transformator input mengisi nilai dalam kurung sudut, seperti `<severity>` dan`<Finding_ID>`, dari jalur Input, jadi Anda tidak perlu menggantinya.

```
{"message":"You have a severity <severity> GuardDuty finding type <Finding_Type> in
 the <region> Region.\n\nFinding Description:\n<Finding_Description>\n\nFor more
 details open the GuardDuty console at https://console.aws.amazon.com/guardduty/
home?region=<region>#/findings?search=id%3D<Finding_ID>"}
```

> **Important**
>
> Berikan template sebagai objek JSON satu baris, dengan pesan dibungkus dalam kunci sepertimessage, seperti yang ditunjukkan pada contoh sebelumnya. Gunakan \n untuk menambahkan jeda baris.
> GuardDuty menemukan bidang seperti `description` dapat berisi karakter kontrol yang tidak dapat diloloskan, termasuk baris baru. Jangan gunakan salah satu format template berikut:
>
> - String yang dikutip telanjang
> - Template multi-baris yang menggunakan string kutipan terpisah pada baris terpisah
>
> Dengan format ini, nilai substitusi dapat menghasilkan JSON yang tidak valid. EventBridge kemudian menolak acara dan tidak mengirimkan pemberitahuan.

> **Note**
>
> Langganan email menerima output template apa adanya, sehingga email menunjukkan objek `message` JSON, dan jeda baris muncul sebagai. \n Untuk notifikasi yang diformat, kirimkan topik Amazon SNS ke Pengembang Amazon Q di aplikasi obrolan (Slack atau Amazon Chime), atau gunakan fungsi Lambda sebagai target.

20. Pilih Konfirmasi.
21. Pilih Berikutnya.
22. (Opsional) Masukkan satu atau lebih tanda untuk aturan. Untuk informasi selengkapnya, lihat EventBridge tag Amazon di Panduan EventBridge Pengguna Amazon.

23. Pilih Berikutnya.
24. Tinjau detail aturan dan pilih Buat aturan.
25. (Opsional) Uji aturan baru Anda dengan menghasilkan temuan sampel dengan proses di Langkah 2. Anda akan menerima email untuk setiap temuan sampel yang dihasilkan.

Langkah selanjutnya

Saat Anda terus menggunakan GuardDuty, Anda akan memahami jenis temuan yang relevan dengan lingkungan Anda. Setiap kali Anda menerima temuan baru, Anda dapat menemukan informasi, termasuk rekomendasi perbaikan tentang temuan itu, dengan memilih Pelajari lebih lanjut dari deskripsi temuan di panel rincian temuan, atau dengan mencari nama temuan di. GuardDuty menemukan jenis

Fitur-fitur berikut akan membantu Anda menyetel GuardDuty sehingga dapat memberikan temuan yang paling relevan untuk AWS lingkungan Anda:

- Untuk mengurutkan temuan dengan mudah berdasarkan kriteria tertentu, seperti ID instans, ID akun, nama bucket S3, dan lainnya, Anda dapat membuat dan menyimpan filter di dalamnya GuardDuty. Untuk informasi selengkapnya, lihat Penyaringan temuan di GuardDuty.
- Jika Anda menerima temuan untuk perilaku yang diharapkan di lingkungan Anda, Anda dapat secara otomatis mengarsipkan temuan berdasarkan kriteria yang Anda tentukan dengan aturan penekanan.
- Untuk mencegah temuan dihasilkan dari subset IP tepercaya, atau memiliki IP GuardDuty monitor di luar lingkup pemantauan normalnya, Anda dapat mengatur IP Tepercaya dan daftar ancaman.

GuardDuty sumber data dasar

GuardDuty menggunakan sumber data dasar untuk mendeteksi komunikasi dengan domain berbahaya dan alamat IP yang diketahui, dan mengidentifikasi perilaku yang berpotensi anomali dan aktivitas yang tidak sah. Saat transit dari sumber-sumber ini ke GuardDuty, semua data log dienkripsi. GuardDuty mengekstrak berbagai bidang dari sumber log ini untuk profil dan deteksi anomali, dan kemudian membuang log ini.

Saat Anda mengaktifkan GuardDuty untuk pertama kalinya di suatu Wilayah, ada uji coba gratis 30 hari yang mencakup deteksi ancaman untuk semua sumber data dasar. Selama uji coba gratis ini, Anda dapat memantau perkiraan penggunaan bulanan yang dirinci oleh setiap sumber data dasar. Sebagai akun GuardDuty administrator yang didelegasikan, Anda dapat melihat perkiraan biaya penggunaan bulanan yang dirinci oleh setiap akun anggota milik organisasi Anda dan telah diaktifkan GuardDuty. Setelah uji coba 30 hari berakhir, Anda dapat menggunakan AWS Billing informasi tentang biaya penggunaan.

Tidak ada biaya tambahan saat GuardDuty mengakses peristiwa dan log dari sumber data dasar ini.

Setelah Anda mengaktifkan GuardDuty di Anda Akun AWS, secara otomatis mulai memantau sumber log yang dijelaskan di bagian berikut. Anda tidak perlu mengaktifkan hal lain GuardDuty untuk mulai menganalisis dan memproses sumber data ini untuk menghasilkan temuan keamanan terkait.

Topik

- AWS CloudTrail acara manajemen
- Log Alur VPC
- Log kueri DNS Route53 Resolver

AWS CloudTrail acara manajemen

AWS CloudTrail memberi Anda riwayat panggilan AWS API untuk akun Anda, termasuk panggilan API yang dilakukan menggunakan Konsol Manajemen AWS, AWS SDK, alat baris perintah, dan AWS layanan tertentu. CloudTrail juga membantu Anda mengidentifikasi pengguna dan akun mana yang memanggil AWS API untuk layanan yang mendukung CloudTrail, alamat IP sumber dari mana panggilan dipanggil, dan waktu panggilan dipanggil. Untuk informasi selengkapnya, lihat Apa yang ada AWS CloudTrail di Panduan AWS CloudTrail Pengguna.

GuardDuty Memantau peristiwa CloudTrail manajemen, juga dikenal sebagai peristiwa bidang kontrol. Peristiwa ini memberikan wawasan tentang operasi manajemen yang dilakukan pada sumber daya di Anda Akun AWS.

Berikut ini adalah contoh peristiwa CloudTrail manajemen yang GuardDuty memantau:

- Mengkonfigurasi keamanan (operasi `AttachRolePolicy` API IAM)
- Mengkonfigurasi aturan untuk merutekan data (operasi Amazon `CreateSubnet` EC2 API)
- Menyiapkan logging (operasi AWS CloudTrail `CreateTrail` API)

Ketika Anda mengaktifkan GuardDuty, itu mulai mengkonsumsi peristiwa CloudTrail manajemen langsung dari CloudTrail melalui aliran peristiwa independen dan duplikat dan menganalisis log CloudTrail peristiwa Anda.

GuardDuty tidak mengelola CloudTrail acara Anda atau memengaruhi CloudTrail konfigurasi yang ada. Demikian pula, CloudTrail konfigurasi Anda tidak memengaruhi cara GuardDuty mengkonsumsi dan memproses log peristiwa. Untuk mengelola akses dan retensi CloudTrail acara Anda, gunakan konsol CloudTrail layanan atau API. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail acara di Panduan AWS CloudTrail Pengguna.

Bagaimana GuardDuty menangani AWS CloudTrail peristiwa global

Untuk sebagian besar AWS layanan, CloudTrail acara dicatat di Wilayah AWS tempat mereka dibuat. Untuk layanan global seperti AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), Amazon CloudFront, dan Amazon Route 53 (Route 53), peristiwa hanya dihasilkan di Wilayah tempat kejadian tetapi memiliki signifikansi global.

Saat GuardDuty mengkonsumsi peristiwa layanan CloudTrail Global (GSE) dengan nilai keamanan seperti konfigurasi jaringan atau izin pengguna, ia mereplikasi peristiwa tersebut dan memprosesnya di setiap Wilayah yang telah Anda aktifkan. GuardDuty Perilaku ini membantu GuardDuty menjaga profil pengguna dan peran di setiap Wilayah, yang sangat penting untuk mendeteksi kejadian anomali.

> **Note**
>
> Untuk temuan yang dihasilkan dari peristiwa layanan global ini, nilai Wilayah dalam temuan mungkin berbeda dari Wilayah tempat GuardDuty membuat deteksi. Misalnya, temuan

mungkin ditampilkan `us-east-1` sebagai Wilayah bahkan jika GuardDuty membuat deteksi di Wilayah yang berbeda.

Kami menyarankan Anda mengaktifkan GuardDuty semua yang Wilayah AWS tersedia di Anda Akun AWS. Bahkan jika Anda tidak memiliki sumber daya yang digunakan di Wilayah tertentu, mengaktifkan akan GuardDuty membantu melindungi akun Anda dari potensi ancaman. Aktor ancaman berpotensi meluncurkan serangan melalui layanan global (seperti IAM, AWS STS, atau Amazon CloudFront). Mereka dapat mencoba membuat sumber daya yang tidak sah untuk mengeksploitasi Wilayah di mana Anda memiliki kehadiran terbatas. GuardDuty memproses peristiwa layanan global di semua Wilayah tempat Anda mengaktifkan layanan, termasuk Wilayah default dan keikutsertaan. Ini membantu GuardDuty mendeteksi aktivitas yang berpotensi mencurigakan di seluruh wilayah Anda Akun AWS, termasuk Wilayah di mana Anda tidak menggunakan sumber daya secara aktif.

Log Alur VPC

Fitur VPC Flow Logs dari Amazon VPC menangkap informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) di lingkungan Anda. AWS

Saat Anda mengaktifkan GuardDuty, segera mulai menganalisis data log aliran VPC dari instans Amazon EC2 dalam akun Anda. GuardDuty mengkonsumsi data ini melalui aliran log aliran independen dan duplikat. Anda tidak perlu membuat atau mengonfigurasi log aliran VPC di akun Anda GuardDuty untuk mengakses data ini. Proses ini tidak memengaruhi konfigurasi log aliran apa pun yang ada.

[Perlindungan Lambda]

Lambda Protection adalah peningkatan opsional untuk Amazon. GuardDuty Saat ini, Pemantauan Aktivitas Jaringan Lambda menyertakan log aliran VPC Amazon dari semua fungsi Lambda untuk akun Anda, bahkan log yang tidak menggunakan jaringan VPC. Untuk melindungi fungsi Lambda Anda dari potensi ancaman keamanan, Anda perlu mengonfigurasi Perlindungan Lambda di akun Anda. GuardDuty Untuk informasi selengkapnya, lihat Perlindungan Lambda.

GuardDuty Pemantauan Runtime

Saat agen GuardDuty keamanan diterapkan pada instans Amazon EC2 dan menerima peristiwa runtime darinya GuardDuty , Anda tidak akan dikenakan biaya Akun AWS untuk menganalisis log aliran VPC dari instance tersebut. Ini menghindari biaya penggunaan ganda.

GuardDuty tidak mengelola log aliran Anda atau membuatnya dapat diakses di akun Anda. Untuk mengelola akses dan retensi log aliran, Anda harus mengonfigurasi fitur VPC Flow Logs.

Log kueri DNS Route53 Resolver

Jika Anda menggunakan resolver AWS DNS untuk instans Amazon EC2 (pengaturan default), maka GuardDuty dapat mengakses dan memproses log kueri DNS Route53 Resolver permintaan dan respons Anda melalui resolver DNS internal. AWS Jika Anda menggunakan resolver DNS lain, seperti OpenDNS atau Googledns, atau jika Anda menyiapkan resolver DNS Anda sendiri, maka tidak dapat mengakses dan memproses data dari sumber data ini. GuardDuty

Saat Anda mengaktifkan GuardDuty, itu segera mulai menganalisis log kueri DNS Route53 Resolver Anda dari aliran data independen. Aliran data ini terpisah dari data yang disediakan melalui fitur pencatatan kueri Route 53 Resolver. Konfigurasi fitur ini tidak mempengaruhi GuardDuty analisis.

> **Note**
>
> GuardDuty tidak mendukung pemantauan log DNS untuk instans Amazon EC2 yang diluncurkan karena fitur pencatatan Amazon Route 53 Resolver kueri tidak tersedia AWS Outposts di lingkungan tersebut.

GuardDuty Deteksi Ancaman yang Diperpanjang

GuardDuty Deteksi Ancaman yang Diperluas secara otomatis mendeteksi serangan multi-tahap yang mencakup sumber data, berbagai jenis AWS sumber daya, dan waktu, dalam. Akun AWS Dengan kemampuan ini, GuardDuty fokus pada urutan beberapa peristiwa yang diamati dengan memantau berbagai jenis sumber data. Deteksi Ancaman yang Diperluas menghubungkan peristiwa ini untuk mengidentifikasi skenario yang menampilkan dirinya sebagai ancaman potensial terhadap AWS lingkungan Anda, dan kemudian menghasilkan temuan urutan serangan.

Topik

- Contoh skenario ancaman urutan serangan
- Cara kerjanya
- Mengaktifkan rencana perlindungan untuk memaksimalkan deteksi ancaman
- Deteksi Ancaman Diperpanjang di GuardDuty konsol
- Memahami dan mengelola temuan urutan serangan
- Sumber daya tambahan

Contoh skenario ancaman urutan serangan

Deteksi Ancaman yang Diperluas mencakup skenario ancaman yang melibatkan kompromi terkait penyalahgunaan AWS kredenSIAL, upaya kompromi data di bucket Amazon S3, dan kompromi sumber daya wadah dan Kubernetes di cluster Amazon EKS. Satu temuan dapat mencakup seluruh urutan serangan. Misalnya, daftar berikut menjelaskan skenario yang GuardDuty mungkin mendeteksi:

Contoh 1 - AWS kredenSIAL dan kompromi data bucket Amazon S3

- Aktor ancaman yang mendapatkan akses tidak sah ke beban kerja komputasi.
- Aktor kemudian melakukan serangkaian tindakan seperti eskalasi hak istimewa dan membangun ketekunan.
- Akhirnya, aktor mengeksfiltrasi data dari sumber daya Amazon S3.

Contoh 2 - Kompromi cluster Amazon EKS

- Aktor ancaman mencoba mengeksploitasi aplikasi kontainer dalam cluster Amazon EKS.
- Aktor menggunakan wadah yang dikompromikan itu untuk mendapatkan token akun layanan istimewa.

- Aktor kemudian memanfaatkan hak istimewa yang ditingkatkan ini untuk mengakses rahasia atau AWS sumber daya Kubernetes yang sensitif melalui identitas pod.

Karena sifat skenario ancaman terkait, GuardDuty anggap semua Jenis pencarian urutan serangan sebagai K ritis.

Video berikut memberikan demonstrasi bagaimana Anda dapat menggunakan Deteksi Ancaman yang Diperpanjang.

Demonstrasi Det GuardDuty eksi Ancaman Diperpanjang Amazon

Cara kerjanya

Saat Anda mengaktifkan Amazon GuardDuty di akun Anda di akun tertentu Wilayah AWS, Deteksi Ancaman yang Diperpanjang juga diaktifkan secara default. Tidak ada biaya tambahan yang terkait dengan penggunaan Deteksi Ancaman yang Diperpanjang. Secara default, ini menghubungkan peristiwa di semuaSumber data dasar. Namun, bila Anda mengaktifkan lebih banyak paket GuardDuty perlindungan, seperti S3 Protection, EKS Protection, dan Runtime Monitoring, ini akan membuka jenis deteksi urutan serangan tambahan dengan memperluas jangkauan sumber peristiwa. Ini berpotensi membantu dengan analisis ancaman yang lebih komprehensif dan deteksi urutan

serangan yang lebih baik. Untuk informasi selengkapnya, lihat Mengaktifkan rencana perlindungan untuk memaksimalkan deteksi ancaman.

GuardDuty menghubungkan beberapa peristiwa, termasuk aktivitas dan GuardDuty temuan API. Peristiwa ini disebut Sin yal. Terkadang, mungkin ada peristiwa di lingkungan Anda yang, dengan sendirinya, tidak menampilkan diri sebagai ancaman potensial yang jelas. GuardDuty menyebutnya sebagai sinyal lemah. Dengan Deteksi Ancaman yang Diperpanjang, GuardDuty mengidentifikasi kapan urutan beberapa tindakan selaras dengan aktivitas yang berpotensi mencurigakan, dan menghasilkan penemuan urutan serangan di akun Anda. Beberapa tindakan ini dapat mencakup sinyal lemah dan GuardDuty temuan yang sudah teridentifikasi di akun Anda.

> **Note**
>
> Saat menghubungkan peristiwa untuk urutan serangan, Deteksi Ancaman yang Diperluas tidak mempertimbangkan temuan yang diarsipkan, termasuk temuan yang diarsipkan secara otomatis karena. Aturan penekanan Perilaku ini memastikan bahwa hanya sinyal aktif dan relevan yang berkontribusi pada deteksi urutan serangan. Untuk memastikan bahwa Anda tidak terpengaruh oleh hal ini, tinjau aturan penekanan yang ada di akun Anda. Untuk informasi selengkapnya, lihat Menggunakan aturan penindasan dengan Deteksi Ancaman yang Diperluas.

GuardDuty juga dirancang untuk mengidentifikasi potensi perilaku serangan yang sedang berlangsung atau baru-baru ini (dalam jendela waktu bergulir 24 jam) di akun Anda. Misalnya, serangan dapat dimulai oleh aktor yang mendapatkan akses yang tidak diinginkan ke beban kerja komputasi. Aktor kemudian akan melakukan serangkaian langkah, termasuk enumerasi, eskalasi hak istimewa, dan eksfiltrasi AWS kredenSIAL. KredenSIAL ini berpotensi digunakan untuk kompromi lebih lanjut atau akses berbahaya ke data.

Mengaktifkan rencana perlindungan untuk memaksimalkan deteksi ancaman

Deteksi Ancaman yang Diperpanjang diaktifkan secara otomatis untuk semua GuardDuty akun, mengevaluasi secara default sinyal dari semua paket perlindungan yang diaktifkan di akun. GuardDuty Sumber data dasar memberikan sinyal penting untuk beberapa deteksi urutan serangan. Misalnya, dengan deteksi ancaman dasar, GuardDuty dapat mengidentifikasi urutan serangan potensial mulai dari aktivitas penemuan hak istimewa IAM di Amazon S3 API, dan mendeteksi

perubahan bidang kontrol S3 berikutnya, seperti perubahan yang membuat kebijakan sumber daya bucket lebih permisif. Namun, urutan serangan lainnya memerlukan sinyal lanjutan yang hanya tersedia dari rencana perlindungan lanjutan seperti pemantauan Runtime, perlindungan S3, dan Pemantauan Log Audit EKS.

Topik

- Mendeteksi urutan serangan di cluster Amazon EKS
- Mendeteksi urutan serangan di bucket Amazon S3
- Mendeteksi urutan serangan di cluster Amazon ECS
- Mendeteksi urutan serangan di grup instans Amazon EC2
- Mendeteksi urutan serangan yang melibatkan beban kerja AI

Mendeteksi urutan serangan di cluster Amazon EKS

GuardDuty mengkorelasikan beberapa sinyal keamanan di seluruh log audit EKS, perilaku proses runtime, dan aktivitas AWS API untuk mendeteksi pola serangan yang canggih. Untuk mendapatkan manfaat dari Deteksi Ancaman yang Diperpanjang untuk EKS, Anda harus mengaktifkan setidaknya satu dari fitur ini - EKS Protection atau Runtime Monitoring (dengan add-on EKS). EKS Protection memantau aktivitas pesawat kontrol melalui log audit, sementara Runtime Monitoring mengamati perilaku di dalam wadah.

Untuk cakupan maksimum dan deteksi ancaman yang komprehensif, GuardDuty disarankan untuk mengaktifkan kedua rencana perlindungan. Bersama-sama, mereka membuat tampilan lengkap cluster EKS Anda, memungkinkan GuardDuty untuk mendeteksi pola serangan yang kompleks. Misalnya, ia dapat mengidentifikasi penyebaran anomali dari wadah istimewa (terdeteksi dengan Perlindungan EKS), diikuti oleh upaya persistensi, penambangan kripto, dan pembuatan shell terbalik dalam wadah itu (terdeteksi dengan Pemantauan Runtime). GuardDuty mewakili peristiwa terkait ini sebagai satu temuan tingkat keparahan kritis, yang disebut. AttackSequence:EKS/CompromisedCluster Saat Anda mengaktifkan kedua rencana perlindungan, pencarian urutan serangan mencakup skenario ancaman berikut:

- Kompromi kontainer yang menjalankan aplikasi web yang rentan
- Akses tidak sah melalui kredensional yang salah konfigurasi
- Upaya untuk meningkatkan hak istimewa
- Permintaan API yang mencurigakan

- Upaya untuk mengakses data dengan jahat

Daftar berikut memberikan rincian saat paket perlindungan khusus ini diaktifkan secara individual:

Perlindungan EKS

Mengaktifkan Perlindungan EKS GuardDuty memberikan kemampuan untuk mendeteksi urutan serangan yang melibatkan aktivitas pesawat kontrol cluster Amazon EKS. Hal ini memungkinkan GuardDuty untuk menghubungkan log audit EKS dan aktivitas AWS API. Misalnya, GuardDuty dapat mendeteksi urutan serangan di mana aktor mencoba akses tidak sah ke rahasia cluster, memodifikasi izin kontrol akses berbasis peran (RBAC) Kubernetes, dan membuat pod istimewa. Untuk informasi selengkapnya tentang mengaktifkan paket perlindungan ini, lihatPerlindungan EKS.

Pemantauan Runtime untuk Amazon EKS

Mengaktifkan Runtime Monitoring untuk cluster Amazon EKS GuardDuty memberikan kemampuan untuk meningkatkan deteksi urutan serangan EKS dengan visibilitas tingkat kontainer. Ini membantu GuardDuty mendeteksi potensi proses berbahaya, perilaku runtime yang mencurigakan, dan eksekusi malware potensial. Misalnya, GuardDuty dapat mendeteksi urutan serangan di mana wadah mulai menunjukkan perilaku yang mencurigakan, seperti proses cryptomining atau membangun koneksi ke titik akhir berbahaya yang diketahui. Untuk informasi selengkapnya tentang mengaktifkan paket perlindungan ini, lihatPemantauan Runtime.

Jika Anda tidak mengaktifkan EKS Protection atau Runtime Monit GuardDuty oring, tidak akan dapat menghasilkan individual Jenis penemuan Perlindungan EKS atau Jenis penemuan Runtime Monitoring. Oleh karena itu, tidak GuardDuty akan dapat mendeteksi urutan serangan multi-tahap yang melibatkan temuan terkait.

Mendeteksi urutan serangan di bucket Amazon S3

Mengaktifkan S3 Protec GuardDuty tion memberikan kemampuan untuk mendeteksi urutan serangan yang melibatkan upaya kompromi data di bucket Amazon S3 Anda. Tanpa Perlindungan S3, GuardDuty dapat mendeteksi kapan kebijakan sumber daya bucket S3 Anda menjadi terlalu permisif. Saat Anda mengaktifkan S3 Protection, GuardDuty memperoleh kemampuan untuk mendeteksi potensi aktivitas eksfiltrasi data yang mungkin terjadi setelah bucket S3 Anda menjadi terlalu permisif.

Jika S3 Protection tidak diaktifkan, tidak GuardDuty akan dapat menghasilkan individualJenis temuan perlindungan S3. Oleh karena itu, tidak GuardDuty akan dapat mendeteksi urutan serangan multi-

tahap yang melibatkan temuan terkait. Untuk informasi selengkapnya tentang mengaktifkan paket perlindungan ini, lihatPerlindungan S3.

Mendeteksi urutan serangan di cluster Amazon ECS

GuardDuty dapat mengidentifikasi urutan serangan seperti proses berbahaya, koneksi ke titik akhir berbahaya, atau perilaku penambangan kripto dalam wadah ECS. Dengan menghubungkan beragam sinyal di seluruh aktivitas jaringan, perilaku proses runtime, dan aktivitas AWS API, GuardDuty dapat mengidentifikasi pola serangan kompleks yang mungkin terlewatkan oleh deteksi individu dan memetakan vektor serangan lengkap.

GuardDuty mewakili peristiwa terkait ini sebagai satu temuan tingkat keparahan kritis, yang disebut. `AttackSequence:ECS/CompromisedCluster` Penemuan urutan serangan mencakup skenario ancaman berikut:

- Kompromi kontainer yang menjalankan layanan rentan
- Eksekusi tidak sah dari alat yang mencurigakan, malware, atau proses cryptomining
- Upaya untuk meningkatkan hak istimewa
- Komunikasi dengan titik akhir yang mencurigakan

> **Important**
>
> Deteksi Ancaman yang Diperpanjang untuk ECS memerlukan Pemantauan Runtime untuk Fargate atau EC2, tergantung pada jenis infrastruktur ECS Anda. Pemantauan Runtime mengamati perilaku dalam wadah ECS yang berjalan pada instans Fargate dan EC2. ECS pada instans EC2 Terkelola tidak didukung.

Mendeteksi urutan serangan di grup instans Amazon EC2

GuardDuty dapat mengidentifikasi urutan serangan yang mempengaruhi instans individual atau grup instans yang memiliki atribut umum seperti grup Penskalaan Otomatis, profil instans IAM, templat peluncuran, tumpu CloudFormation kan, AMI, atau ID VPC. Instans ini mungkin menunjukkan perilaku mencurigakan seperti proses berbahaya, koneksi ke titik akhir berbahaya, penambangan kripto, atau penggunaan kredentif instans EC2 yang tidak normal.

Penemuan urutan serangan mendeteksi skenario ancaman berikut:

- Kompromi instans yang menjalankan layanan rentan
- Penggunaan kredentif instans Amazon EC2 yang diperoleh melalui IMDS dari luar AWS akun tempat kredensialnya dikeluarkan
- Gunakan sebagai infrastruktur untuk serangan seperti proxy, pemindaian, atau penolakan layanan
- Eksekusi tidak sah dari alat yang mencurigakan, malware, atau proses cryptomining
- Komunikasi dengan titik akhir yang mencurigakan

Deteksi Ancaman yang Diperluas membantu mengidentifikasi ancaman ini. GuardDuty mewakili peristiwa terkait ini sebagai satu temuan tingkat keparahan kritis, yang disebut. `AttackSequence:EC2/CompromisedInstanceGroup`

Untuk meningkatkan Deteksi Ancaman yang Diperluas untuk kemampuan deteksi EC2, aktifkan Runtime Monitoring. Kombinasi fundamental GuardDuty, yang memantau CloudTrail dan aktivitas jaringan, dan Pemantauan Runtime, yang mengamati perilaku proses dan panggilan sistem dalam instance, memberikan deteksi ancaman yang lebih komprehensif. Pemantauan terintegrasi ini memungkinkan GuardDuty untuk mendeteksi urutan serangan canggih seperti akses tidak sah melalui kredenSIAL yang salah dikonfigurasi, upaya eskalasi hak istimewa, dan akses tidak sah ke data sensitif. Dengan menghubungkan beragam sinyal ini, GuardDuty dapat mengidentifikasi pola serangan kompleks yang mungkin terlewatkan oleh deteksi individu dan memetakan vektor serangan lengkap.

Mendeteksi urutan serangan yang melibatkan beban kerja AI

Akti Perlindungan AI fkan untuk membantu GuardDuty mendeteksi urutan serangan yang mengancam beban kerja AI di akun Anda. AI Protection menganalisis peristiwa AWS CloudTrail data dari Amazon Bedrock dan Amazon SageMaker AI. Ini dapat mendeteksi aktivitas seperti pemanggilan model anomali, serangan biaya panen, dan upaya injeksi cepat langsung.

Untuk menambahkan sinyal dari beban kerja AI Anda ke urutan AttackSequence:IAM/CompromisedCredentials serangan, Anda harus mengaktifkan Perlindungan AI. GuardDutykemudian dapat menggunakan jenis temuan berikut sebagai sinyal korelasi:

- Impact:IAMUser/AnomalousModelInvocation
- Impact:IAMUser/CostHarvesting
- Impact:IAMUser/PromptInjection.Direct

Misalnya, aktor ancaman mungkin menggunakan AWS kredenSIAL yang berpotensi dikompromikan yang sama untuk membuat pemanggilan model Amazon Bedrock atau Amazon SageMaker AI yang tidak normal. GuardDuty dapat mengkorelasikan pemanggilan itu dengan tindakan mencurigakan lainnya yang diambil dengan kredenSIAL tersebut. Ini kemudian mewakili mereka sebagai penemuan urutan AttackSequence:IAM/CompromisedCredentials serangan tunggal. Dengan sendirinya, temuan Perlindungan AI tidak menghasilkan urutan serangan.

Jika Perlindungan AI tidak diaktifkan, GuardDuty tidak dapat menghasilkan individualJenis penemuan Perlindungan AI. Akibatnya, GuardDuty tidak dapat mendeteksi urutan serangan multi-tahap yang melibatkan temuan ini. Untuk informasi selengkapnya tentang mengaktifkan paket perlindungan ini, lihatPerlindungan AI.

Deteksi Ancaman Diperpanjang di GuardDuty konsol

Secara default, halaman Deteksi Ancaman yang Diper GuardDuty luas di konsol menampilkan Status sebagai Di aktifkan. Dengan deteksi ancaman dasar, status mewakili bahwa GuardDuty dapat mendeteksi urutan serangan potensial yang melibatkan aktivitas penemuan hak istimewa IAM di API Amazon S3 dan mendeteksi perubahan bidang kontrol S3 berikutnya.

Gunakan langkah-langkah berikut untuk mengakses halaman Deteksi Ancaman yang Diperluas di GuardDuty konsol:

1. Anda dapat membuka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi kiri, pilih Deteksi An caman yang Diperpanjang.

   Halaman ini memberikan rincian tentang skenario ancaman yang dicakup oleh Deteksi Ancaman Diperpanjang.
3. Pada halaman Det eksi Ancaman yang Diperluas, lihat bagian Paket perlindungan terkait. Jika Anda ingin mengaktifkan paket perlindungan khusus untuk meningkatkan cakupan deteksi ancaman di akun Anda, pilih opsi Konfigurasi untuk paket perlindungan tersebut.

Memahami dan mengelola temuan urutan serangan

Temuan urutan serangan sama seperti GuardDuty temuan lain di akun Anda. Anda dapat melihatnya di halaman Temuan di GuardDuty konsol. Untuk informasi tentang melihat temuan, lihatHalaman temuan di GuardDuty konsol.

Mirip dengan GuardDuty temuan lain, temuan urutan serangan juga secara otomatis dikirim ke Amazon EventBridge. Berdasarkan pengaturan Anda, temuan urutan serangan juga diekspor ke tujuan penerbitan (bucket Amazon S3). Untuk menetapkan tujuan penerbitan baru atau memperbarui yang sudah ada, lihatMengekspor temuan yang dihasilkan ke Amazon S3.

Sumber daya tambahan

Lihat bagian berikut untuk mendapatkan pemahaman lebih lanjut tentang urutan serangan:

- Setelah mempelajari tentang Deteksi Ancaman yang Diperluas dan urutan serangan, Anda dapat menghasilkan jenis pencarian urutan serangan sampel dengan mengikuti langkah-langkah diSampel temuan.
- Pelajari tentang Jenis pencarian urutan serangan.
- Tinjau temuan dan jelajahi detail temuan yang terkait dengannyaDetail pencarian urutan serangan.
- Prioritaskan dan atasi jenis pencarian urutan serangan dengan mengikuti langkah-langkah untuk sumber daya terkait yang terkena dampak diMengatasi temuan.

Mengkonfigurasi rencana perlindungan

Halaman Paket Perlindungan di GuardDuty konsol menggabungkan semua konfigurasi paket perlindungan ke dalam satu halaman. Anda dapat mengaktifkan atau menonaktifkan paket perlindungan, mengonfigurasi pengaturan aktifkan otomatis untuk AWS Organizations akun, dan melihat statistik akun anggota dari satu lokasi.

Ikhtisar

Halaman Paket Perlindungan terpadu menggantikan kebutuhan untuk menavigasi ke halaman paket perlindungan individual untuk konfigurasi. Navigasi konsol menampilkan satu tautan Paket Perlindungan.

Halaman ini menampilkan rencana perlindungan dalam urutan sebagai berikut:

1. Dasar GuardDuty - Aktifkan atau nonaktifkan GuardDuty dan konfigurasikan aktifkan otomatis untuk AWS Organizations akun.
2. Perlindungan S3 - Pantau peristiwa data Amazon S3 untuk potensi ancaman terhadap data Anda.
3. Runtime Monitoring - Memantau peristiwa tingkat sistem operasi untuk beban kerja EKS, ECS, dan EC2.
4. Log Audit EKS — Pantau log audit Amazon EKS untuk potensi ancaman terhadap klaster Anda.
5. Perlindungan RDS — Memantau aktivitas login RDS untuk potensi ancaman ke database Anda.
6. Perlindungan Lambda - Memantau aktivitas jaringan fungsi Lambda untuk potensi ancaman.

Setiap paket perlindungan menampilkan informasi berikut:

- Status fitur (Diaktifkan atau Tidak diaktifkan)
- Auto-enable status untuk AWS Organizations akun
- AWS Organizations statistik anggota akun

Mengkonfigurasi semua rencana perlindungan

Untuk mengonfigurasi paket perlindungan dari halaman terpadu, gunakan langkah-langkah berikut:

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

2. Di panel navigasi, pilih Paket Perlindungan.
3. Pilih Konfigurasikan semua enablements. Semua wadah rencana perlindungan beralih ke mode edit.
4. Buat perubahan di setiap atau semua rencana perlindungan. Untuk setiap paket, Anda dapat mengaktifkan atau menonaktifkan fitur dan mengonfigurasi pengaturan aktifkan otomatis untuk akun organisasi.
5. Pilih Simpan semua. Modal konfirmasi muncul merangkum semua perubahan, termasuk nama fitur, status, dan nilai aktifkan otomatis untuk setiap paket yang dimodifikasi.
6. Tinjau perubahan dan pilih Konfirmasi dan simpan. Semua perubahan disimpan dalam batch.

Auto-enable pilihan

Setiap paket perlindungan menyediakan opsi aktifkan otomatis berikut untuk akun organisasi:

Aktifkan untuk semua akun

Aktifkan fitur untuk semua GuardDuty akun aktif di organisasi. Ini termasuk akun baru yang bergabung dengan organisasi.

Aktifkan untuk akun baru

Ini akan berlaku untuk setiap akun baru ketika mereka ditambahkan ke organisasi.

Jangan aktifkan secara otomatis

Fitur ini tidak diaktifkan secara otomatis untuk akun organisasi.

Untuk GuardDuty wadah Foundational, opsi aktifkan otomatis menggunakan kata-kata AWS Organizations-spesifik:

- Aktifkan untuk semua AWS Organizations akun — Aktifkan GuardDuty untuk semua akun aktif di akun Anda AWS Organizations.
- Aktifkan untuk AWS Organizations akun baru — Ini akan berlaku untuk setiap akun baru ketika mereka ditambahkan ke akun Anda AWS Organizations.

Konfigurasi Runtime Monitoring

Container Runtime Monitoring memiliki struktur induk-anak dengan sub-fitur berikut:

- Pemantauan Runtime (EKS)
- Pemantauan Runtime (ECS)
- Pemantauan Runtime (EC2)

Pengaturan Runtime Monitoring Infrastructure ditampilkan di bagian yang dapat diperluas. Pengaturan ini diperlukan agar Runtime Monitoring untuk EKS, ECS, dan EC2 berfungsi tetapi tidak memberikan perlindungan sendiri.

Kendala dua arah

Sub-fitur dan infrastruktur Runtime Monitoring memiliki hubungan berikut:

Aktifkan sub-fitur

Secara otomatis mengaktifkan Infrastruktur Pemantauan Runtime jika dinonaktifkan.

Nonaktifkan sub-fitur

Tidak berpengaruh pada Infrastruktur Pemantauan Runtime.

Aktifkan Infrastruktur Pemantauan Runtime

Tidak berpengaruh pada sub-fitur.

Nonaktifkan Infrastruktur Pemantauan Runtime

Menonaktifkan semua sub-fitur.

Untuk pengaturan aktifkan otomatis, batasan berikut berlaku:

Naikkan auto-enable sub-fitur

Infrastruktur Pemantauan Runtime selalu sama dengan maksimum semua sub-fitur.

Turunkan auto-enable sub-fitur

Runtime Monitoring Infrastructure menghitung ulang hingga maksimum baru dari semua sub-fitur.

Naikkan aktifkan otomatis Infrastruktur Pemantauan Runtime

Tidak berpengaruh pada sub-fitur.

Aktifkan otomatis Infrastruktur Pemantauan Runtime yang lebih rendah

Menurunkan sub-fitur apa pun yang melebihi nilai induk baru agar sesuai dengannya.

> **Note**
>
> Peringatan muncul ketika sub-fitur apa pun memiliki nilai yang berbeda dari Infrastruktur Pemantauan Runtime (baik sakelar atau aktifkan ketidakcocokan otomatis). Mengaktifkan hanya Runtime Monitoring Infrastructure menempatkan Anda dalam mode manual tanpa manajemen otomatis agen keamanan. Aktifkan Runtime Monitoring untuk EKS, ECS, atau EC2 untuk secara otomatis mengelola agen keamanan untuk beban kerja Anda.

Statistik organisasi

Setiap wadah paket perlindungan menampilkan statistik akun anggota yang menunjukkan berapa banyak akun yang mengaktifkan fitur tersebut. Ketika statistik organisasi belum tersedia (misalnya, dalam 24 jam pertama setelah mengaktifkan), halaman menampilkan indikator status tertunda dengan pesan yang menjelaskan bahwa statistik sedang dikumpulkan.

Integrasi halaman akun

Tombol Edit di bagian aktifkan otomatis pada halaman Akun mengarahkan Anda ke halaman Rencana Perlindungan alih-alih membuka modal konfigurasi lama.

GuardDuty Perlindungan AI

GuardDuty AI Protection memperluas deteksi GuardDuty ancaman Amazon ke beban kerja AI bawaan. AWS Saat Anda mengaktifkan Perlindungan AI, GuardDuty analisis peristiwa AWS CloudTrail data dari Amazon Bedrock, Amazon Bedrock, AgentCore dan Amazon SageMaker AI, bersama dengan AWS CloudTrail peristiwa manajemen. GuardDuty menggunakan data ini untuk mendeteksi aktivitas yang berpotensi mencurigakan yang menargetkan model pondasi dan aplikasi yang memanggilnya. Ketika GuardDuty mengidentifikasi ancaman potensial, itu menghasilkan satu atau lebihJenis penemuan Perlindungan AI.

Saat Anda mengaktifkan Perlindungan AI, GuardDuty dapat mendeteksi jenis ancaman berikut:

- Pemanggilan anomali dari Amazon Bedrock atau SageMaker Amazon AI model yang menyimpang dari baseline yang ditetapkan untuk identitas atau akun, seperti pemanggilan dari alamat IP yang tidak biasa, API yang tidak biasa, atau model yang tidak biasa.
- Serangan panen biaya, di mana aktor ancaman mengirimkan input yang mahal secara komputasi ke model Amazon Bedrock atau SageMaker Amazon AI untuk meningkatkan konsumsi token dan biaya operasi akun.
- Upaya injeksi cepat langsung, di mana aktor ancaman membuat permintaan jahat untuk membuat model pondasi mengabaikan instruksi aslinya. Deteksi ini memerlukan Amazon Bedrock Guardrails dan hanya berlaku untuk beban kerja Amazon Bedrock.

> **Note**
>
> Jenis temuan yang GuardDuty dapat dihasilkan Wilayah AWS bergantung pada layanan AI mana yang tersedia di Wilayah tersebut:
>
> - Jenis Impact:IAMUser/AnomalousModelInvocation dan Impact:IAMUser/CostHarvesting temuan membutuhkan Amazon Bedrock atau Amazon SageMaker AI. Di Wilayah di mana Amazon Bedrock tidak tersedia, GuardDuty hasilkan jenis temuan ini hanya dari pemanggilan model Amazon SageMaker AI.
> - Jenis Impact:IAMUser/PromptInjection.Direct temuan membutuhkan Amazon Bedrock Guardrails. Ini tidak tersedia di Wilayah di mana Amazon Bedrock Guardrails tidak didukung.

Untuk daftar Wilayah di mana setiap jenis temuan didukung, lihatRegion-specific ketersediaan fitur.

Tip

Untuk mendapatkan nilai keamanan maksimal dari Perlindungan AI, terapkan Amazon Bedrock Guardrails untuk serangan cepat di semua akun di organisasi Anda. AWS Gunakan kebijakan AWS Organizations Amazon Bedrock untuk mengelola pengaturan pagar pembatas ini secara terpusat. Ini memungkinkan perlindungan seragam di semua akun dengan kontrol dan manajemen terpusat. Ketika pagar pembatas serangan cepat diberlakukan, GuardDuty buat temuan injeksi yang cepat. Untuk informasi selengkapnya, lihat Impact:IAMUser/PromptInjection.Direct.

Untuk mendeteksi ancaman terhadap beban kerja AI Anda, Anda harus mengaktifkan Perlindungan AI di GuardDuty akun Anda. Untuk informasi tentang mengaktifkan Perlindungan AI, lihat Mengaktifkan Perlindungan AI di lingkungan multi-akun untuk lingkungan multi-akun atau. Mengaktifkan Perlindungan AI untuk akun mandiri

Topik

- Bagaimana AI Protection bekerja
- Harga untuk Perlindungan AI
- Deteksi ancaman tambahan untuk beban kerja AI
- Mengaktifkan Perlindungan AI di lingkungan multi-akun
- Mengaktifkan Perlindungan AI untuk akun mandiri

Bagaimana AI Protection bekerja

Saat Anda mengaktifkan Perlindungan AI untuk akun atau di seluruh organisasi Anda, GuardDuty secara otomatis mulai mengumpulkan peristiwa AWS CloudTrail data dari layanan AI di akun yang dipantau. Anda tidak perlu membuat jejak, mengaktifkan pencatatan peristiwa data, atau membuat perubahan apa pun pada aplikasi AI Anda.

Untuk mengumpulkan peristiwa data, GuardDuty buat saluran AWS CloudTrail terkait layanan di setiap akun yang dipantau. Saluran terkait layanan mengalirkan peristiwa AWS CloudTrail data untuk Amazon Bedrock, Amazon Bedrock, dan Amazon AgentCore AI, dan SageMaker sumber daya AI GuardDuty terkait untuk analisis. Karena GuardDuty membuat dan mengelola saluran ini:

- GuardDuty mengonfigurasi setelan peristiwa data saluran, dan pemilik akun tidak dapat memodifikasinya. Ini berarti deteksi ancaman tidak bergantung pada pemilik akun yang mengonfigurasi atau memelihara jejak.
- Setiap akun yang dipantau dapat mengonfirmasi bahwa saluran aktif di CloudTrail konsol (di bawah Pengaturan, Service-linkedsaluran) atau dengan memanggil operasi AWS CloudTrail ListChannelsAPI.

GuardDuty menggunakan dua metode deteksi untuk menghasilkan temuan Perlindungan AI, tergantung pada jenis temuan:

- Untuk jenis Impact:IAMUser/AnomalousModelInvocation dan Impact:IAMUser/CostHarvesting temuan, GuardDuty gunakan model pembelajaran mesin deteksi anomali (ML) untuk menganalisis peristiwa yang dikumpulkan dan menetapkan dasar aktivitas pemanggilan model normal untuk setiap identitas IAM dan. Akun AWS GuardDuty menghasilkan temuan ketika mendeteksi aktivitas yang menyimpang secara signifikan dari baseline ini.
- Untuk jenis Impact:IAMUser/PromptInjection.Direct temuan, buat temuan saat Amazon Bedrock Guardrails mengevaluasi prompt dan mendeteksi serangan cepat, berdasarkan peristiwa data yang GuardDuty dihasilkan. AWS CloudTrail

Untuk informasi selengkapnya tentang peristiwa AWS CloudTrail data, lihat Mencatat peristiwa data di Panduan AWS CloudTrail Pengguna.

Harga untuk Perlindungan AI

Saat Anda mengaktifkan Perlindungan GuardDuty AI, GuardDuty biaya untuk volume peristiwa AWS CloudTrail data yang dianalisis, diukur dalam GB. GuardDuty membuat saluran terkait layanan tanpa CloudTrail biaya tambahan kepada Anda. Biaya pengumpulan peristiwa data ini sudah termasuk dalam biaya penggunaan Perlindungan AI Anda. Anda juga terus dikenakan biaya penggunaan standar untuk GuardDuty dan paket perlindungan lain yang diaktifkan. Untuk harga dan contoh saat ini, lihat GuardDuty harga Amazon.

Deteksi ancaman tambahan untuk beban kerja AI

Selain rencana Perlindungan AI, paket Amazon GuardDuty Foundational dan Lambda Protection menawarkan deteksi untuk membantu Anda mengamankan dan mendeteksi ancaman terhadap beban kerja AI yang ada di dalamnya. AWS

Rencana GuardDuty Foundational memantau peristiwa AWS CloudTrail manajemen untuk mendeteksi aktivitas mencurigakan dan berbahaya dalam beban kerja AI yang dibuat dengan menggunakan AWS layanan, termasuk Amazon Bedrock dan Amazon AI. SageMaker Misalnya, GuardDuty dapat mengidentifikasi kegiatan seperti:

- Penghapusan pagar keamanan Amazon Bedrock yang tidak biasa
- Perubahan pada sumber data pelatihan model yang berpotensi menyebabkan serangan keracunan data
- Pencatatan dinonaktifkan untuk pemanggilan model Amazon Bedrock yang mungkin menunjukkan upaya untuk menghindari deteksi
- Contoh notebook yang tidak biasa atau pelatihan penciptaan lapangan kerja di Amazon SageMaker AI
- Kredensi Amazon Elastic Compute Cloud yang diekstraksi yang mungkin telah digunakan untuk memanggil API di Amazon Bedrock, Amazon AI, atau beban kerja SageMaker AI yang dikelola sendiri di instans Amazon EC2, kluster Amazon EKS, atau tugas Amazon ECS.

GuardDuty Lambda Protection dapat membantu mendeteksi potensi ancaman yang terkait dengan agen Amazon Bedrock. Ini mungkin termasuk aktivitas jaringan yang mencurigakan seperti cryptomining, dan komunikasi dengan server perintah dan kontrol berbahaya. Ancaman ini dapat disebabkan oleh serangan rantai pasokan atau dorongan kompleks.

Mengaktifkan Perlindungan AI di lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan Perlindungan AI untuk akun anggota di organisasi. Akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka sendiri. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota menggunakan AWS Organizations, dan dapat memilih untuk mengaktifkan Perlindungan AI secara otomatis untuk semua akun baru saat mereka bergabung dengan organisasi. Untuk informasi selengkapnya tentang lingkungan beberapa akun, lihat Mengelola beberapa akun di Amazon. GuardDuty

Mengaktifkan Perlindungan AI untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan AI untuk akun GuardDuty administrator yang didelegasikan.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Paket Perlindungan.
3. Pilih Konfigurasikan semua enablements. Di bawah Perlindungan AI, Anda dapat melihat status konfigurasi Perlindungan AI saat ini.
4. Lakukan salah satu tindakan berikut:

   Penggunaan Aktifkan untuk semua akun

   - Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
   - Pilih Simpan.

   Penggunaan Konfigurasikan akun secara manual

   - Untuk mengaktifkan paket perlindungan hanya untuk akun akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
   - Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
   - Pilih Simpan.

API/CLI

Jalankan operasi UpdateDetectorAPI menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek `name` sebagai `AI_PROTECTION` dan `status` sebagai `ENABLED` atau`DISABLED`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut memungkinkan Perlindungan AI untuk akun GuardDuty administrator yang didelegasikan. Ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan AI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name": "AI_PROTECTION", "Status": "ENABLED"}]'
```

Untuk menonaktifkan Perlindungan AI, ganti `ENABLED` dengan`DISABLED`.

Mengaktifkan Perlindungan AI untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan AI untuk semua akun anggota aktif yang ada di organisasi.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensil akun GuardDuty administrator yang didelegasikan.
2. Di panel navigasi, pilih Paket Perlindungan.
3. Pilih Konfigurasikan semua enablements. Di bawah Perlindungan AI, di bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
5. Pilih Simpan.

API/CLI

Untuk mengaktifkan atau menonaktifkan Perlindungan AI secara selektif untuk akun anggota Anda, jalankan operasi UpdateMemberDetectorsAPI menggunakan milik Anda sendiri*detector ID*.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut memungkinkan Perlindungan AI untuk satu akun anggota. Untuk menonaktifkannya, ganti `ENABLED` dengan `DISABLED`. Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --region us-east-1 --features '[{"Name":
 "AI_PROTECTION", "Status": "ENABLED"}]'
```

Ketika perintah berjalan dengan sukses, ia mengembalikan daftar kosongUnprocessedAccounts. Jika ada masalah mengubah pengaturan detektor untuk akun, respons mencantumkan ID akun tersebut bersama dengan ringkasan masalah.

Auto-enable Perlindungan AI untuk akun anggota baru

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan AI untuk akun baru yang bergabung dengan organisasi Anda.

Di konsol, akun GuardDuty administrator yang didelegasikan dapat mengaktifkan Perlindungan AI secara otomatis untuk akun anggota baru dengan menggunakan halaman Paket Perlindungan atau halaman Akun.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensil akun GuardDuty administrator yang didelegasikan.
2. Lakukan salah satu tindakan berikut:
   - Menggunakan halaman Paket Perlindungan:
     1. Di panel navigasi, pilih Paket Perlindungan.
     2. Pilih Konfigurasikan semua enablements.
     3. Di bawah Perlindungan AI, pilih Konfigurasi akun secara manual, lalu pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, GuardDuty secara otomatis mengaktifkan Perlindungan AI untuk akun itu. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
     4. Pilih Simpan.
   - Menggunakan halaman Akun:
     1. Di panel navigasi, pilih Akun.
     2. Pada halaman Akun, pilih Auto-enablepreferensi.

3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Perlindungan AI.
4. Pilih Simpan.

API/CLI

Untuk mengaktifkan Perlindungan AI untuk akun anggota baru, jalankan operasi UpdateOrganizationConfigurationAPI menggunakan milik Anda sendiri*detector ID*.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut memungkinkan Perlindungan AI untuk akun baru yang bergabung dengan organisasi Anda. Jika Anda tidak ingin mengaktifkannya untuk semua akun baru, setel `AutoEnable` ke`NONE`.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features
 '[{"Name": "AI_PROTECTION", "AutoEnable": "NEW"}]'
```

Mengaktifkan Perlindungan AI untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di AWS akunnya di Wilayah tertentu.

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations atau melalui undangan, bagian ini tidak berlaku untuk Anda. Untuk informasi tentang mengelola beberapa akun, lihatMengaktifkan Perlindungan AI di lingkungan multi-akun.

Setelah Anda mengaktifkan Perlindungan AI, GuardDuty mulailah memantau aktivitas pemanggilan model Amazon Bedrock dan Amazon SageMaker AI yang dikumpulkannya untuk akun Anda. CloudTrail

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan AI di akun mandiri Anda.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

2. Dari pemilih Wilayah di sudut kanan atas, pilih Wilayah tempat Anda ingin mengaktifkan Perlindungan AI.
3. Di panel navigasi, pilih Paket Perlindungan.
4. Pilih Konfigurasikan semua enablements. Di bawah Perlindungan AI, pilih Aktifkan untuk mengaktifkan Perlindungan AI.
5. Pilih Simpan semua, lalu pilih Konfirmasi dan simpan.

API/CLI

Jalankan operasi UpdateDetectorAPI menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek `name` sebagai `AI_PROTECTION` dan `status` sebagai`ENABLED`.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan AI. Jalankan perintah berikut, dan ganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan ID detektor akun Anda dan *`us-east-1`* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan AI.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name": "AI_PROTECTION", "Status": "ENABLED"}]'
```

Untuk menonaktifkan Perlindungan AI, ganti `ENABLED` dengan`DISABLED`.

GuardDuty Perlindungan EKS

> **Note**
>
> Anda dapat mengonfigurasi Perlindungan EKS bersama dengan semua paket perlindungan lainnya dari satu halaman di GuardDuty konsol. Untuk informasi selengkapnya, lihat Mengkonfigurasi rencana perlindungan.

EKS Protection membantu Anda mendeteksi potensi risiko keamanan di klaster Amazon Elastic Kubernetes Service (Amazon EKS) di lingkungan Anda. AWS Misalnya, ini membantu Anda mendeteksi ketika klaster EKS yang salah dikonfigurasi diakses oleh aktor yang tidak diautentikasi yang mencoba mengumpulkan rahasia atau AWS kredensil dari cluster Anda. EKS Protection menggunakan log audit EKS untuk menganalisis aktivitas pengguna dan aplikasi.

Saat Anda mengaktifkan Perlindungan EKS, GuardDuty secara otomatis mulai memantau kluster Amazon EKS Anda untuk potensi ancaman keamanan. GuardDuty menggunakan aliran independennya sendiri untuk mengumpulkan dan menganalisis Log audit EKS di Perlindungan EKS — tidak diperlukan konfigurasi tambahan.

Ketika GuardDuty mendeteksi potensi ancaman berdasarkan pemantauan log audit EKS, itu menghasilkan temuan keamanan. Untuk informasi tentang jenis temuan yang GuardDuty mungkin dihasilkan saat Anda mengaktifkan Perlindungan EKS, lihatJenis penemuan Perlindungan EKS.

> **Note**
>
> Untuk melihat log audit EKS di akun Anda (opsional), Anda dapat mengonfigurasi pencatatan bidang kontrol Amazon EKS untuk mengirim log audit ke CloudWatch Log. Konfigurasi ini terpisah dari Perlindungan EKS dan tidak diperlukan untuk kemampuan pemantauan keamanan di GuardDuty.

Uji coba gratis 30 hari

- Ketika Anda mengaktifkan GuardDuty Akun AWS in an Wilayah AWS untuk pertama kalinya, Anda mendapatkan uji coba gratis 30 hari. Dalam hal ini, juga GuardDuty akan mengaktifkan Perlindungan EKS, yang termasuk dalam uji coba gratis 30 hari.

- Ketika Anda sudah menggunakan GuardDuty dan memutuskan untuk mengaktifkan Perlindungan EKS untuk pertama kalinya, akun Anda di Wilayah ini akan mendapatkan uji coba gratis 30 hari untuk Perlindungan EKS.
- Anda dapat memilih untuk menonaktifkan Perlindungan EKS di Wilayah mana pun kapan saja.
- Selama uji coba gratis 30 hari, Anda bisa mendapatkan perkiraan biaya penggunaan Anda di akun dan Wilayah tersebut. Setelah uji coba gratis 30 hari berakhir, GuardDuty tidak secara otomatis menonaktifkan Perlindungan EKS. Akun Anda di Wilayah ini akan mulai menimbulkan biaya penggunaan. Untuk informasi selengkapnya, lihat Memantau penggunaan dan memperkirakan biaya.

Saat Anda menonaktifkan Perlindungan EKS, GuardDuty segera berhenti memantau dan menganalisis log audit EKS untuk sumber daya Amazon EKS Anda.

Perlindungan EKS mungkin tidak tersedia di semua Wilayah AWS tempat GuardDuty yang tersedia. Untuk informasi selengkapnya, lihat Region-specific ketersediaan fitur.

> **Note**
>
> EKS Runtime Monitoring dikelola sebagai bagian dari Runtime Monitoring. Untuk informasi selengkapnya, lihat GuardDuty Pemantauan Runtime.

Log audit EKS di Perlindungan EKS

Log audit EKS menangkap tindakan berurutan dalam klaster Amazon EKS Anda, termasuk aktivitas dari pengguna, aplikasi yang menggunakan Kubernetes API, dan control plane. Audit logging adalah komponen dari semua klaster Kubernetes.

Untuk informasi selengkapnya, lihat Auditing dalam dokumentasi Kubernetes.

Amazon EKS memungkinkan log audit EKS untuk dicerna sebagai CloudWatch Log Amazon melalui fitur pencatatan bidang kontrol EKS. GuardDuty tidak mengelola pencatatan pesawat kontrol Amazon EKS Anda atau membuat log audit EKS dapat diakses di akun Anda jika Anda belum mengaktifkannya untuk Amazon EKS. Untuk mengelola akses dan retensi log audit EKS Anda, Anda harus mengonfigurasi fitur pencatatan bidang kontrol Amazon EKS. Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan log bidang kontrol di Panduan Pengguna Amazon EKS.

Mengaktifkan Perlindungan EKS di lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengaktifkan atau menonaktifkan Perlindungan EKS; fitur untuk akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan ini dapat memilih untuk mengaktifkan Perlindungan EKS secara otomatis untuk semua akun baru saat mereka bergabung dengan organisasi. Untuk informasi selengkapnya tentang lingkungan beberapa akun, lihat Mengelola beberapa akun di Amazon. GuardDuty

Mengkonfigurasi EKS Audit Log Monitoring untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengonfigurasi Pemantauan Log Audit EKS untuk akun GuardDuty administrator yang didelegasikan.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Paket Perlindungan.
3. Pilih Konfigurasikan semua aktivasi. Di bawah EKS Audit Log, Anda dapat melihat status konfigurasi EKS Audit Log Monitoring saat ini.
4. Lakukan salah satu tindakan berikut:

   Menggunakan Aktifkan untuk semua akun

   - Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
   - Pilih Simpan.

   Menggunakan Konfigurasi akun secara manual

   - Untuk mengaktifkan paket perlindungan hanya untuk akun akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
   - Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).

- Pilih Simpan.

API/CLI

Jalankan operasi updateDetectorAPI menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek `name` sebagai `EKS_AUDIT_LOGS` dan `status` sebagai `ENABLED` atau`DISABLED`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Anda dapat mengaktifkan atau menonaktifkan EKS Audit Log Monitoring dengan menjalankan AWS CLI perintah berikut. Pastikan untuk menggunakan akun GuardDuty administrator yang didelegasikan valid*`detector ID`*.

> **Note**
>
> Kode contoh berikut memungkinkan EKS Audit Log Monitoring. Pastikan untuk mengganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan akun administrator `detector-id` yang didelegasikan dan *`555555555555`* dengan akun GuardDuty administrator Akun AWS yang didelegasikan GuardDuty .

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name": "EKS_AUDIT_LOGS", "Status": "ENABLED"}]'
```

Untuk menonaktifkan EKS Audit Log Monitoring, ganti `ENABLED` dengan`DISABLED`.

Auto-enable EKS Audit Log Monitoring untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Log Audit EKS untuk akun anggota yang ada di organisasi Anda.

Console

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu tindakan berikut:

   Menggunakan halaman Rencana Perlindungan

   1. Di panel navigasi, pilih Paket Perlindungan.
   2. Pilih Konfigurasikan semua aktivasi. Di bawah Log Audit EKS, Anda dapat melihat status Pemantauan Log Audit EKS saat ini untuk akun anggota aktif di organisasi Anda.
   3. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan Pemantauan Log Audit EKS untuk akun yang ada dan yang baru di organisasi.
   4. Pilih Simpan semua, lalu pilih Konfirmasi dan simpan.

   > **Note**
   >
   > Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

   Menggunakan halaman Akun

   1. Di panel navigasi, pilih Akun.
   2. Pada halaman Akun, pilih Auto-enablepreferensi sebelum Tambahkan akun berdasarkan undangan.
   3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah Pemantauan Log Audit EKS.
   4. Pilih Simpan.

   Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun dan ingin menyesuaikan konfigurasi Pemantauan Log Audit EKS untuk akun tertentu di organisasi Anda, lihatAktifkan atau nonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun anggota.

API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri*detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan EKS Audit Log Monitoring untuk satu akun anggota. Untuk menonaktifkannya, ganti `ENABLED` dengan `DISABLED`.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Pemantauan Log Audit EKS untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Log Audit EKS untuk semua akun anggota aktif yang ada di organisasi.

Console

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.
2. Di panel navigasi, pilih Paket Perlindungan.
3. Pilih Konfigurasikan semua aktivasi. Di bawah Log Audit EKS, di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.

5. Pilih Simpan.

API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri*detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan EKS Audit Log Monitoring untuk satu akun anggota. Untuk menonaktifkannya, ganti `ENABLED` dengan `DISABLED`.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Auto-enable EKS Audit Log Monitoring untuk akun anggota baru

Akun anggota yang baru ditambahkan harus Aktifkan GuardDuty sebelum memilih mengonfigurasi pemindaian GuardDuty-initiated malware. Akun anggota yang dikelola oleh undangan dapat mengonfigurasi pemindaian GuardDuty-initiated malware secara manual untuk akun mereka. Untuk informasi selengkapnya, lihat Step 3 - Accept an invitation.

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Log Audit EKS untuk akun baru yang bergabung dengan organisasi Anda.

Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan Pemantauan Log Audit EKS untuk akun anggota baru dalam suatu organisasi, baik menggunakan halaman Pemantauan Log Audit EKS atau Akun.

Untuk mengaktifkan Pemantauan Log Audit EKS secara otomatis untuk akun anggota baru

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.
2. Lakukan salah satu tindakan berikut:
   - Menggunakan halaman Paket Perlindungan:
     1. Di panel navigasi, pilih Paket Perlindungan.
     2. Pilih Konfigurasikan semua aktivasi. Di bawah EKS Audit Logs, konfigurasikan pengaturan auto-enable.
     3. Pilih Konfigurasikan akun secara manual.
     4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, Pemantauan Log Audit EKS akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
     5. Pilih Simpan.
   - Menggunakan halaman Akun:
     1. Di panel navigasi, pilih Akun.
     2. Pada halaman Akun, pilih Auto-enablepreferensi.
     3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Pemantauan Log Audit EKS.
     4. Pilih Simpan.

API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun baru Anda, jalankan operasi UpdateOrganizationConfigurationAPI menggunakan milik Anda sendiri*`detector ID`*.

- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan EKS Audit Log Monitoring untuk anggota baru yang bergabung dengan organisasi Anda. Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
   "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
  ```

Aktifkan atau nonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS untuk akun anggota selektif di organisasi Anda.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.
2. Di panel navigasi, pilih Akun.

   Pada halaman Akun, tinjau kolom Pemantauan Log Audit EKS untuk status akun anggota Anda.
3. Untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS

   Pilih akun yang ingin Anda konfigurasi untuk EKS Audit Log Monitoring. Anda dapat memilih beberapa akun sekaligus. Di bawah dropdown Edit Protection Plans, pilih EKS Audit Log Monitoring, lalu pilih opsi yang sesuai.

API/CLI

Untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *`detector ID`*

Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan EKS Audit Log Monitoring untuk satu akun anggota. Untuk menonaktifkannya, ganti `ENABLED` dengan `DISABLED`. Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

Mengaktifkan Perlindungan EKS untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di AWS akun mereka di Wilayah tertentu.

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk Anda. Untuk informasi tentang mengelola beberapa akun, lihatMengaktifkan Perlindungan EKS di lingkungan multi-akun.

Setelah Anda mengaktifkan Perlindungan EKS, GuardDuty akan mulai memantau log audit EKS untuk kluster Amazon EKS di akun Anda.

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan EKS di akun mandiri Anda.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Dari pemilih Wilayah di sudut kanan atas, pilih Wilayah tempat Anda ingin mengaktifkan Perlindungan EKS.
3. Di panel navigasi, pilih Paket Perlindungan.
4. Pilih Konfigurasikan semua aktivasi. Di bawah Log Audit EKS, pilih Aktifkan untuk mengaktifkan Perlindungan EKS.
5. Pilih Simpan semua, lalu pilih Konfirmasi dan simpan.

API/CLI

- Jalankan operasi updateDetectorAPI menggunakan ID detektor regional dari akun GuardDuty administrator yang didelegasikan dan meneruskan nama `features` objek sebagai `EKS_AUDIT_LOGS` dan status sebagai`ENABLED`.

  Atau, Anda juga dapat mengaktifkan Perlindungan EKS menjalankan AWS CLI perintah. Jalankan perintah berikut, dan ganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan ID detektor akun Anda dan *`us-east-1`* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan EKS.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  region us-east-1 --features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
  ```

GuardDuty Perlindungan S3

> **Note**
>
> Anda dapat mengonfigurasi Perlindungan S3 bersama dengan semua paket perlindungan lainnya dari satu halaman di GuardDuty konsol. Untuk informasi selengkapnya, lihat Mengkonfigurasi rencana perlindungan.

S3 Protection membantu Anda mendeteksi potensi risiko keamanan untuk data, seperti eksfiltrasi dan penghancuran data, di bucket Amazon Simple Storage Service (Amazon S3). GuardDuty memantau peristiwa AWS CloudTrail data untuk Amazon S3, yang mencakup operasi API tingkat objek untuk mengidentifikasi risiko ini di semua bucket Amazon S3 di akun Anda.

Ketika GuardDuty mendeteksi potensi ancaman berdasarkan pemantauan peristiwa data S3, itu menghasilkan temuan keamanan. Untuk informasi tentang jenis temuan yang GuardDuty mungkin dihasilkan saat Anda mengaktifkan Perlindungan S3, lihatGuardDuty Jenis temuan perlindungan S3.

Secara default, deteksi ancaman dasar mencakup pemantauan AWS CloudTrail acara manajemen untuk mengidentifikasi potensi ancaman di sumber daya Amazon S3 Anda. Sumber data ini berbeda dari peristiwa AWS CloudTrail data untuk S3 karena keduanya memantau berbagai jenis aktivitas di lingkungan Anda.

Anda dapat mengaktifkan Perlindungan S3 di akun di Wilayah mana pun yang GuardDuty mendukung fitur ini. Ini akan membantu Anda memantau peristiwa CloudTrail data untuk S3 di akun dan Wilayah itu. Setelah Anda mengaktifkan Perlindungan S3, Anda GuardDuty akan dapat sepenuhnya memantau bucket Amazon S3 Anda dan menghasilkan temuan untuk akses mencurigakan ke data yang disimpan di bucket S3 Anda.

Untuk menggunakan Perlindungan S3, Anda tidak perlu secara eksplisit mengaktifkan atau mengonfigurasi login peristiwa data S3. AWS CloudTrail

Uji coba gratis 30 hari

Daftar berikut menjelaskan bagaimana uji coba gratis 30 hari akan bekerja untuk akun Anda:

- Saat Anda mengaktifkan GuardDuty di Wilayah baru untuk pertama kalinya, Anda mendapatkan uji coba gratis 30 hari. Akun AWS Dalam hal ini, juga GuardDuty akan mengaktifkan Perlindungan S3, yang termasuk dalam uji coba gratis.

- Ketika Anda sudah menggunakan GuardDuty dan memutuskan untuk mengaktifkan Perlindungan S3 untuk pertama kalinya, akun Anda di Wilayah ini akan mendapatkan uji coba gratis 30 hari untuk Perlindungan S3.
- Anda dapat memilih untuk menonaktifkan Perlindungan S3 di Wilayah mana pun kapan saja.
- Selama uji coba gratis 30 hari, Anda bisa mendapatkan perkiraan biaya penggunaan Anda di akun dan Wilayah tersebut. Setelah uji coba gratis 30 hari berakhir, Perlindungan S3 tidak dinonaktifkan secara otomatis. Akun Anda di Wilayah ini akan mulai menimbulkan biaya penggunaan. Untuk informasi selengkapnya, lihat Memantau GuardDuty Penggunaan dan Memperkirakan Biaya.

AWS CloudTrail peristiwa data untuk S3

Peristiwa data, juga dikenal sebagai operasi bidang data, memberikan wawasan tentang operasi sumber daya yang dilakukan pada atau di dalam sumber daya. Operasi ini sering kali merupakan aktivitas bervolume tinggi.

Berikut ini adalah contoh peristiwa CloudTrail data untuk S3 yang GuardDuty dapat memantau:

- Operasi API `GetObject`
- Operasi API `PutObject`
- Operasi API `ListObjects`
- Operasi API `DeleteObject`

Untuk informasi selengkapnya tentang API ini, lihat Referensi API Amazon Simple Storage Service.

Cara GuardDuty menggunakan peristiwa CloudTrail data untuk S3

Saat Anda mengaktifkan Perlindungan S3, GuardDuty mulailah menganalisis peristiwa CloudTrail data untuk S3 dari semua bucket S3 Anda, dan memantaunya untuk aktivitas berbahaya dan mencurigakan. Untuk informasi selengkapnya, lihat AWS CloudTrail acara manajemen.

Ketika pengguna yang tidak diautentikasi mengakses objek S3, itu berarti bahwa objek S3 dapat diakses publik. Oleh karena itu, GuardDuty tidak memproses permintaan tersebut. GuardDuty memproses permintaan yang dibuat ke objek S3 dengan menggunakan kredenal IAM (AWS Identity and Access Management) atau AWS STS (AWS Security Token Service) yang valid.

> **Catatan**
>
> Setelah mengaktifkan Perlindungan S3, GuardDuty memantau peristiwa data dari bucket Amazon S3 yang berada di Wilayah yang sama tempat Anda mengaktifkan. GuardDuty

Jika Anda menonaktifkan Perlindungan S3 di akun Anda di Wilayah tertentu, GuardDuty menghentikan pemantauan peristiwa data S3 dari data yang disimpan di bucket S3 Anda. GuardDuty tidak akan lagi menghasilkan jenis pencarian Perlindungan S3 untuk akun Anda di Wilayah tersebut.

GuardDuty menggunakan peristiwa CloudTrail data untuk S3 untuk urutan serangan

GuardDuty Deteksi Ancaman yang Diperpanjangmendeteksi urutan serangan multi-tahap yang menjangkau sumber data dasar, sumber AWS daya, dan garis waktu, dalam sebuah akun. Saat GuardDuty mengamati urutan peristiwa yang menunjukkan aktivitas mencurigakan baru-baru ini atau sedang berlangsung di akun Anda, buat temuan urutan serangan GuardDuty terkait.

Secara default, saat Anda mengaktifkan GuardDuty, Extended Threat Detection juga diaktifkan di akun Anda. Kemampuan ini mencakup skenario ancaman yang terkait dengan peristiwa CloudTrail manajemen tanpa biaya tambahan. Namun, untuk menggunakan Extended Threat Detection pada potensi penuhnya, GuardDuty merekomendasikan untuk mengaktifkan Perlindungan S3 untuk mencakup skenario ancaman yang terkait dengan peristiwa CloudTrail data untuk S3.

Setelah Anda mengaktifkan Perlindungan S3, secara otomatis GuardDuty akan mencakup skenario ancaman urutan serangan, seperti kompromi atau penghancuran data, di mana sumber daya Amazon S3 Anda mungkin terlibat.

Mengaktifkan Perlindungan S3 di lingkungan beberapa akun

Dalam lingkungan multi-akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengonfigurasi (mengaktifkan atau menonaktifkan) Perlindungan S3 untuk akun anggota di organisasi mereka. AWS Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan dapat memilih untuk mengaktifkan Perlindungan S3 secara otomatis di semua akun, hanya akun baru, atau tidak ada akun di organisasi. Untuk informasi selengkapnya, lihat Mengelola akun dengan AWS Organizations.

Mengaktifkan Perlindungan S3 untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 untuk akun GuardDuty administrator yang didelegasikan.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Perlindungan S3.
3. Pada halaman Perlindungan S3, pilih Edit.
4. Lakukan salah satu tindakan berikut:

   Menggunakan Aktifkan untuk semua akun

   - Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
   - Pilih Simpan.

   Menggunakan Konfigurasi akun secara manual

   - Untuk mengaktifkan paket perlindungan hanya untuk akun akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
   - Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
   - Pilih Simpan.

API/CLI

Jalankan updateDetectordengan menggunakan ID detektor akun GuardDuty administrator yang didelegasikan untuk Wilayah saat ini dan meneruskan `features` objek `name` sebagai `S3_DATA_EVENTS` dan `status` sebagai`ENABLED`.

Atau, Anda dapat mengkonfigurasi Perlindungan S3 dengan menggunakan AWS Command Line Interface. Jalankan perintah berikut, dan pastikan untuk mengganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan ID detektor akun GuardDuty administrator yang didelegasikan untuk Wilayah saat ini.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name": "S3_DATA_EVENTS", "Status": "ENABLED"}]'
```

Auto-enable Perlindungan S3 untuk semua akun anggota di organisasi

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 untuk akun GuardDuty administrator yang didelegasikan.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Masuk menggunakan akun akun administrator Anda.
2. Lakukan salah satu tindakan berikut:

   Menggunakan halaman Perlindungan S3

   1. Di panel navigasi, pilih Perlindungan S3.
   2. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis mengaktifkan Perlindungan S3 untuk akun yang ada dan baru di organisasi.
   3. Pilih Simpan.

   > **Note**
   >
   > Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

   Menggunakan halaman Akun

   1. Di panel navigasi, pilih Akun.
   2. Pada halaman Akun, pilih Auto-enablepreferensi sebelum Tambahkan akun berdasarkan undangan.
   3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah Perlindungan S3.

4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun, lihatAktifkan Perlindungan S3 secara selektif di akun anggota.

API/CLI

- Untuk mengaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID*
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Pastikan untuk mengganti *12abc34d567e8fa901bc2d34e56789f0* dengan akun GuardDuty administrator `detector-id` yang didelegasikan, dan*111122223333*.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Perlindungan S3 untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 untuk semua akun anggota aktif yang ada di organisasi Anda.

Console

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Perlindungan S3.
3. Pada halaman Perlindungan S3, Anda dapat melihat status konfigurasi saat ini. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
5. Pilih Konfirmasi.

API/CLI

- Untuk mengaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *`detector ID`*
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Pastikan untuk mengganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan akun GuardDuty administrator `detector-id` yang didelegasikan, dan*`111122223333`*.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Auto-enable Perlindungan S3 untuk akun anggota baru

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 untuk akun baru yang bergabung dengan organisasi Anda.

Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan akun anggota baru di organisasi melalui konsol, menggunakan halaman Perlindungan S3 atau Akun.

Untuk mengaktifkan Perlindungan S3 secara otomatis untuk akun anggota baru

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensil akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu tindakan berikut:
   - Menggunakan halaman Perlindungan S3:
     1. Di panel navigasi, pilih Perlindungan S3.
     2. Pada halaman Perlindungan S3, pilih Edit.
     3. Pilih Konfigurasikan akun secara manual.
     4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, Perlindungan S3 akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
     5. Pilih Simpan.
   - Menggunakan halaman Akun:
     1. Di panel navigasi, pilih Akun.
     2. Pada halaman Akun, pilih Auto-enablepreferensi.
     3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Perlindungan S3.
     4. Pilih Simpan.

API/CLI

- Untuk mengaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, jalankan operasi UpdateOrganizationConfigurationAPI menggunakan milik Anda sendiri. *`detector ID`*
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Tetapkan preferensi untuk mengaktifkan atau menonaktifkan paket perlindungan secara otomatis di Wilayah tersebut untuk akun baru (`NEW`) yang bergabung dengan organisasi,

semua akun (`ALL`), atau tidak ada akun (`NONE`) di organisasi. Untuk informasi selengkapnya, lihat auto EnableOrganizationMembers. Berdasarkan preferensi Anda, Anda mungkin perlu mengganti `NEW` dengan `ALL` atau`NONE`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Perlindungan S3 secara selektif di akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 secara selektif untuk akun anggota.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensil akun GuardDuty administrator yang didelegasikan.
2. Di panel navigasi, pilih Akun.

   Pada halaman Akun, tinjau kolom Perlindungan S3 untuk status akun anggota Anda.
3. Untuk mengaktifkan Perlindungan S3 secara selektif

   Pilih akun yang ingin Anda aktifkan Perlindungan S3. Anda dapat memilih beberapa akun sekaligus. Di menu dropdown Edit Protection Plans, pilih S3Pro, lalu pilih opsi yang sesuai.

API/CLI

Untuk mengaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan ID detektor Anda sendiri. Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Untuk menonaktifkannya, ganti `true` dengan `false`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
 aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features
 '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

> **Note**
>
> Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

> **Note**
>
> Jika Anda menggunakan skrip untuk mengaktifkan akun baru dan ingin menonaktifkan Perlindungan S3 di akun baru, Anda dapat memodifikasi operasi createDetectorAPI dengan `dataSources` objek opsional seperti yang dijelaskan dalam topik ini.

Mengaktifkan Perlindungan S3 untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat Mengaktifkan Perlindungan S3 di lingkungan beberapa akun.

Setelah Anda mengaktifkan Perlindungan S3, GuardDuty akan mulai memantau peristiwa AWS CloudTrail data untuk bucket S3 di akun Anda.

Pilih metode akses pilihan Anda untuk mengonfigurasi Perlindungan S3 untuk akun mandiri.

Console

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Dari pemilih Wilayah di sudut kanan atas, pilih Wilayah tempat Anda ingin mengaktifkan Perlindungan S3.
3. Di panel navigasi, pilih Perlindungan S3.
4. Halaman Perlindungan S3 memberikan status Perlindungan S3 saat ini untuk akun Anda. Pilih Aktifkan atau Nonaktifkan untuk mengaktifkan atau menonaktifkan Perlindungan S3 kapan saja.
5. Pilih Konfirmasi untuk mengonfirmasi pilihan Anda.

API/CLI

Jalankan updateDetectordengan menggunakan ID detektor valid Anda untuk Wilayah saat ini dan meneruskan `features` objek `name` yang `S3_DATA_EVENTS` disetel `ENABLED` untuk mengaktifkan Perlindungan S3, masing-masing.

> **Note**
>
> Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Atau, Anda dapat menggunakan AWS Command Line Interface. Untuk mengaktifkan Perlindungan S3, jalankan perintah berikut, dan ganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan ID detektor akun Anda dan *`us-east-1`* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan S3.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

GuardDuty Pemantauan Runtime

> **Note**
>
> Anda dapat mengonfigurasi Runtime Monitoring bersama dengan semua paket perlindungan lainnya dari satu halaman di GuardDuty konsol. Untuk informasi selengkapnya, lihat Mengkonfigurasi rencana perlindungan.

Runtime Monitoring mengamati dan menganalisis tingkat sistem operasi, jaringan, dan peristiwa file untuk membantu Anda mendeteksi potensi ancaman dalam beban kerja tertentu AWS di lingkungan Anda.

AWS Sumber daya yang didukung dalam Runtime Monitoring — Runtime Monitoring menyediakan cakupan deteksi ancaman untuk Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Service (Amazon ECS) on, dan Amazon Elastic Compute Cloud (Amazon AWS Fargate EC2) resource.

GuardDuty tidak mendukung kluster Amazon EKS yang berjalan AWS Fargate.

Dalam dokumen ini dan bagian lain yang terkait dengan Runtime Monitoring, GuardDuty gunakan terminologi jenis sumber daya untuk merujuk ke Amazon EKS, Fargate Amazon ECS, dan sumber daya Amazon EC2.

Runtime Monitoring menggunakan agen GuardDuty keamanan yang menambahkan visibilitas ke dalam perilaku runtime, seperti akses file, eksekusi proses, argumen baris perintah, dan koneksi jaringan. Untuk setiap jenis sumber daya yang ingin Anda pantau untuk potensi ancaman, Anda dapat mengelola agen keamanan untuk jenis sumber daya tertentu baik secara otomatis atau manual (dengan pengecualian untuk Fargate (hanya Amazon ECS)). Mengelola agen keamanan secara otomatis berarti Anda mengizinkan GuardDuty untuk menginstal dan memperbarui agen keamanan atas nama Anda. Di sisi lain, ketika Anda mengelola agen keamanan untuk sumber daya Anda secara manual, Anda bertanggung jawab untuk menginstal dan memperbarui agen keamanan, sesuai kebutuhan.

Dengan kemampuan yang diperluas ini, GuardDuty dapat membantu Anda mengidentifikasi dan merespons potensi ancaman yang dapat menargetkan aplikasi dan data yang berjalan di beban kerja dan instance pribadi Anda. Misalnya, ancaman berpotensi dimulai dengan mengorbankan satu

wadah yang menjalankan aplikasi web yang rentan. Aplikasi web ini mungkin memiliki izin akses ke wadah dan beban kerja yang mendasarinya. Dalam skenario ini, kredensil yang tidak dikonfigurasi dengan benar berpotensi menyebabkan akses yang lebih luas ke akun, dan data yang tersimpan di dalamnya.

Dengan menganalisis peristiwa runtime dari setiap kontainer dan beban kerja, GuardDuty berpotensi mengidentifikasi kompromi kontainer dan AWS kredenal terkait pada fase awal, dan mendeteksi upaya untuk meningkatkan hak istimewa, permintaan API yang mencurigakan, dan akses berbahaya ke data di lingkungan Anda.

Daftar Isi

- Cara kerjanya
- Bagaimana cara kerja uji coba gratis 30 hari di Runtime Monitoring
- Prasyarat untuk mengaktifkan Pemantauan Runtime
- Mengaktifkan GuardDuty Runtime Monitoring
- Mengelola agen GuardDuty keamanan
- Meninjau statistik cakupan runtime dan masalah pemecahan masalah
- Menyiapkan CPU dan pemantauan memori
- Menggunakan VPC bersama dengan Runtime Monitoring
- Menggunakan Infrastructure as Code (IAc) dengan GuardDuty agen keamanan otomatis
- Jenis acara runtime yang dikumpulkan yang menggunakan GuardDuty
- Agen hosting repositori Amazon ECR GuardDuty
- Dua agen keamanan pada host yang mendasari yang sama
- Pemantauan Runtime EKS di GuardDuty
- GuardDuty versi rilis agen keamanan
- Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring

Cara kerjanya

Runtime Monitoring menggunakan agen keamanan ringan untuk mengamati perilaku runtime Amazon EC2, Amazon EKS, dan Amazon ECS Anda pada beban kerja Fargate dan mendeteksi ancaman. Ia bekerja ujung ke ujung sebagai berikut:

1. Agen dikerahkan ke sumber daya Anda. GuardDuty dapat menyebarkan dan memperbarui agen untuk Anda (konfigurasi agen otomatis), atau Anda dapat menerapkan dan mengelolanya sendiri (konfigurasi agen manual). Langkah-langkahnya tergantung pada jenis sumber daya.
2. Agen mengumpulkan acara runtime. Pada setiap sumber daya yang dipantau, agen mengamati aktivitas tingkat sistem operasi, seperti eksekusi proses, akses file, dan koneksi jaringan.
3. Agen mengirimkan acara ke GuardDuty. Agen mengirimkan acara ke GuardDuty backend. Data tetap berada dalam AWS jaringan, dan GuardDuty tidak mengenakan biaya untuk peristiwa yang dikirimkan dari sumber daya komputasi Anda ke GuardDuty. Lihat perinciannya di Bagaimana agen keamanan terhubung ke GuardDuty.
4. GuardDuty menganalisis peristiwa dan menghasilkan temuan. Ketika mendeteksi perilaku mencurigakan, seperti eskalasi hak istimewa atau komunikasi dengan host jahat yang dikenal, GuardDuty menghasilkan temuan. Untuk melihat daftar temuan terbaru yang GuardDuty dihasilkan, lihatGuardDuty Jenis penemuan Runtime Monitoring.

Agen berjalan dalam batas CPU dan memori yang ditentukan, sehingga konsumsi sumber dayanya tetap dapat diprediksi dan tidak menurunkan kinerja atau ketersediaan beban kerja yang berjalan pada host yang sama. Untuk batasan ini, lihatPrasyarat untuk mengaktifkan Pemantauan Runtime.

Daftar Isi

- Mengaktifkan Runtime Monitoring
- Menyebarkan agen keamanan ke Amazon EKS
- Menyebarkan agen keamanan ke Amazon EC2
- Menyebarkan agen keamanan ke Amazon ECS di Fargate
- Bagaimana agen keamanan terhubung ke GuardDuty
- Melacak cakupan Pemantauan Runtime

Mengaktifkan Runtime Monitoring

Mengaktifkan Runtime Monitoring adalah proses dua langkah:

1. Aktifkan Runtime Monitoring untuk akun Anda. GuardDuty kemudian menerima peristiwa runtime dari instans Amazon EC2, kluster Amazon ECS, dan beban kerja Amazon EKS.
2. Kelola agen GuardDuty keamanan untuk sumber daya yang ingin Anda pantau. Berdasarkan jenis sumber daya, Anda dapat:

- Gunakan konfigurasi agen otomatis — GuardDuty menyebarkan agen dan menetapkan konektivitasnya.
- Kelola agen secara manual - Anda membuat titik akhir VPC dan mengelola instalasi dan pembaruan agen.

Mengelola agen berbeda menurut jenis sumber daya. Untuk detailnya, lihat:

- Menyebarkan agen keamanan ke Amazon EKS
- Menyebarkan agen keamanan ke Amazon EC2
- Menyebarkan agen keamanan ke Amazon ECS di Fargate

Saat agen GuardDuty keamanan diterapkan pada instans Amazon EC2 dan menerima peristiwa runtime darinya GuardDuty , Anda tidak akan dikenakan biaya Akun AWS untuk menganalisis log aliran VPC dari instance tersebut. Ini menghindari biaya penggunaan ganda.

Menyebarkan agen keamanan ke Amazon EKS

GuardDuty Runtime Monitoring memantau kluster Amazon EKS Anda untuk ancaman dengan menyebarkan agen GuardDuty keamanan kepada mereka. Di Amazon EKS, GuardDuty menyebarkan agen sebagai add-on `aws-guardduty-agent` EKS.

> **Catatan**
>
> Runtime Monitoring mendukung klaster Amazon EKS yang berjalan di instans Amazon EC2 dan Mode Otomatis Amazon EKS.
> Runtime Monitoring tidak mendukung kluster Amazon EKS dengan Amazon EKS Hybrid Nodes, dan yang berjalan. AWS Fargate
> Untuk informasi tentang fitur Amazon EKS ini, lihat Apa itu Amazon EKS? di Panduan Pengguna Amazon EKS.

Anda dapat membiarkan GuardDuty mengelola agen secara otomatis (disarankan) atau mengelolanya secara manual.

Konfigurasi agen otomatis (disarankan)

GuardDuty mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS Anda. Di GuardDuty konsol, konfigurasi ini muncul sebagai Runtime Monitoring (EKS).

Untuk bagaimana agen keamanan terhubung GuardDuty, lihatBagaimana agen keamanan terhubung ke GuardDuty.

Dampak memungkinkan agen keamanan

GuardDuty menyebarkan agen keamanan ke kluster EKS Anda, dan Amazon Elastic Kubernetes Service (Amazon EKS) mengoordinasikan penerapannya ke node.

Lingkup pemantauan

Secara default, GuardDuty mengelola agen keamanan untuk semua kluster EKS di akun Anda, termasuk cluster baru yang Anda buat. Untuk berhenti GuardDuty mengelola agen pada klaster tertentu, tambahkan tag`GuardDutyManaged`: `false` ke cluster itu.

Untuk informasi selengkapnya tentang menandai kluster EKS, lihat Menandai resource Amazon EKS Anda di Panduan Pengguna Amazon EKS.

Pertimbangan-pertimbangan

- Ketika konfigurasi agen otomatis dimatikan, GuardDuty mengelola agen keamanan hanya pada kluster EKS yang Anda tag dengan`GuardDutyManaged`:`true`.
- Menambahkan `false` tag`GuardDutyManaged`: berhenti GuardDuty mengelola agen keamanan, tetapi tidak menghapus instalan agen yang sudah diinstal.
- Lindungi `GuardDutyManaged` tag dengan mengontrol siapa yang dapat memodifikasinya, menggunakan kebijakan kontrol layanan atau kebijakan IAM. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan (SCP) di Panduan AWS Organizations Pengguna atau Kontrol akses ke AWS sumber daya di Panduan Pengguna IAM.

Konfigurasi agen manual

Gunakan pendekatan ini ketika Anda ingin menyebarkan dan mengelola agen GuardDuty keamanan secara manual di semua kluster EKS Anda. Pastikan Runtime Monitoring diaktifkan untuk akun Anda. Agen GuardDuty keamanan mungkin tidak berfungsi seperti yang diharapkan jika Runtime Monitoring tidak diaktifkan.

Dampak menggunakan pendekatan ini

Anda harus mengoordinasikan penyebaran agen GuardDuty keamanan dalam kluster EKS Anda di semua akun Anda. Untuk mendapatkan fitur keamanan terbaru, Anda juga harus memperbarui agen saat GuardDuty merilis versi baru. Untuk informasi selengkapnya tentang versi agen untuk EKS, lihatGuardDuty versi agen keamanan untuk sumber daya Amazon EKS.

Pertimbangan-pertimbangan

Anda harus mendukung aliran data yang aman sambil memantau dan mengatasi kesenjangan cakupan karena klaster dan beban kerja baru terus digunakan.

Topik terkait

- Bagaimana agen keamanan terhubung ke GuardDuty
- Melacak cakupan Pemantauan Runtime

Menyebarkan agen keamanan ke Amazon EC2

GuardDuty Runtime Monitoring memantau instans Amazon EC2 Anda untuk ancaman dengan menerapkan agen keamanan ke instans Amazon EC2 Anda GuardDuty .

> **Note**
>
> Runtime Monitoring juga mengumpulkan peristiwa runtime dari tugas Amazon ECS yang berjalan di instans Amazon EC2 Anda.

Anda dapat membiarkan GuardDuty mengelola agen secara otomatis (disarankan) atau mengelolanya secara manual.

Konfigurasi agen otomatis (disarankan)

GuardDuty mengelola penyebaran dan pembaruan ke agen keamanan untuk instans Amazon EC2 Anda. Di GuardDuty konsol, konfigurasi ini muncul sebagai Runtime Monitoring (EC2).

Untuk bagaimana agen keamanan terhubung GuardDuty, lihatBagaimana agen keamanan terhubung ke GuardDuty.

Dampak memungkinkan agen keamanan

Dengan konfigurasi agen otomatis, GuardDuty buat satu asosiasi SSM untuk instans SSM-managed Amazon EC2 Anda (ditampilkan di bawah Fleet Manager di https://console.aws.amazon.com/systems-manager/konsol) dan menggunakannya untuk menginstal dan memperbarui agen.

Lingkup pemantauan

Secara default, GuardDuty mengelola agen keamanan untuk semua instans Amazon EC2 di akun Anda. Untuk berhenti GuardDuty mengelola agen pada instance tertentu, tambahkan tag`GuardDutyManaged`: `false` ke instance itu.

Pertimbangan-pertimbangan

- Ketika konfigurasi agen otomatis dimatikan, GuardDuty mengelola agen keamanan hanya pada instans Amazon EC2 yang Anda tag dengan:. `GuardDutyManaged` `true`
- Menambahkan `false` tag`GuardDutyManaged`: berhenti GuardDuty mengelola agen keamanan, tetapi tidak menghapus instalan agen yang sudah diinstal.
- Lindungi `GuardDutyManaged` tag dengan mengontrol siapa yang dapat memodifikasinya, menggunakan kebijakan kontrol layanan atau kebijakan IAM. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan (SCP) di Panduan AWS Organizations Pengguna atau Kontrol akses ke AWS sumber daya di Panduan Pengguna IAM.

Konfigurasi agen manual

Ada dua cara untuk mengelola agen keamanan untuk Amazon EC2 secara manual:

- Untuk instans SSM-managed Amazon EC2, Anda dapat menggunakan dokumen GuardDuty terkelola AWS Systems Manager untuk menginstal agen keamanan.

  > **Note**
  >
  > Untuk menggunakan opsi ini, pastikan setiap instans Amazon EC2 baru yang Anda luncurkan diaktifkan SSM.

- Gunakan skrip pengelola paket RPM (RPM) untuk menginstal agen keamanan di instans Amazon EC2 Anda, terlepas dari apakah itu dikelola SSM atau tidak.

Topik terkait

- Bagaimana agen keamanan terhubung ke GuardDuty
- Melacak cakupan Pemantauan Runtime

Menyebarkan agen keamanan ke Amazon ECS di Fargate

GuardDuty Runtime Monitoring memantau kluster Amazon ECS Anda di Fargate untuk ancaman dengan menyebarkan agen keamanan kepada mereka. GuardDuty

> **Note**
>
> Runtime Monitoring tidak mendukung aplikasi yang berjalan di Instans Terkelola Amazon ECS.

GuardDuty mengelola agen secara otomatis; manajemen manual tidak tersedia untuk Fargate. Di GuardDuty konsol, konfigurasi ini muncul sebagai Runtime Monitoring (ECS).

Konfigurasi agen otomatis (disarankan)

GuardDuty mengelola penyebaran dan pembaruan ke agen keamanan untuk tugas Fargate baru di kluster Amazon ECS Anda.

Untuk bagaimana agen keamanan terhubung GuardDuty, lihatBagaimana agen keamanan terhubung ke GuardDuty.

Dampak memungkinkan agen keamanan

Untuk setiap tugas Fargate baru, GuardDuty lampirkan kontainer sespan yang menjalankan agen keamanan dan mengumpulkan peristiwa runtime dari kontainer dalam tugas tersebut.

Gambar sespan disimpan di Amazon Elastic Container Registry (Amazon ECR) Registry ECR), dengan lapisan di Amazon S3, dan ditarik saat tugas dimulai. Bergantung pada konfigurasi jaringan Anda, Anda mungkin perlu mengizinkan akses ke ECR dan S3. Misalnya, izinkan daftar awalan terkelola S3 jika Anda menggunakan grup keamanan terbatas. Untuk informasi selengkapnya, lihat Prasyarat untuk akses gambar kontainer.

Jika sespan tidak dapat diluncurkan, Runtime Monitoring tidak mencegah tugas berjalan. Tugas Fargate tidak dapat dimodifikasi setelah dimulai, jadi GuardDuty lampirkan sespan saat peluncuran tugas.

Lingkup pemantauan

Secara default, GuardDuty mengelola agen keamanan untuk semua cluster Amazon ECS di akun Anda. Untuk berhenti GuardDuty mengelola agen pada klaster tertentu, tambahkan tag`GuardDutyManaged`: `false` ke cluster itu.

Untuk informasi lebih lanjut tentang mengelola agen untuk tugas Fargate, lihat. Mengelola agen keamanan otomatis untuk Fargate (hanya Amazon ECS)

Pertimbangan-pertimbangan

- Saat konfigurasi agen otomatis dinonaktifkan, GuardDuty mengelola agen keamanan hanya di kluster Amazon ECS yang Anda beri tag:. `GuardDutyManaged` `true`
- Menambahkan `false` tag`GuardDutyManaged`: berhenti GuardDuty mengelola agen keamanan, tetapi tidak menghapus instalan agen yang sudah diinstal.
- Lindungi `GuardDutyManaged` tag dengan mengontrol siapa yang dapat memodifikasinya, menggunakan kebijakan kontrol layanan atau kebijakan IAM. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan (SCP) di Panduan AWS Organizations Pengguna atau Kontrol akses ke AWS sumber daya di Panduan Pengguna IAM.

Topik terkait

- Bagaimana agen keamanan terhubung ke GuardDuty
- Melacak cakupan Pemantauan Runtime

Bagaimana agen keamanan terhubung ke GuardDuty

Agen keamanan Runtime Monitoring mengirimkan acara runtime ke. GuardDuty Data tetap berada di dalam AWS jaringan. Tidak ada biaya tambahan untuk konektivitas yang GuardDuty dikonfigurasi. Untuk mengautentikasi agen, GuardDuty gunakan peran identitas Instance. Untuk Amazon ECS di Fargate GuardDuty , gunakan peran eksekusi tugas; lihat. Persyaratan izin

GuardDuty mendukung dua metode konektivitas: link-local dan titik akhir Amazon VPC. Agen keamanan mencoba untuk terhubung menggunakan metode ini untuk mengirimkan peristiwa runtime ke GuardDuty.

Dengan konfigurasi agen otomatis, GuardDuty menetapkan konektivitas secara otomatis. Jika Anda mengelola agen secara manual, Anda perlu membuat titik akhir VPC Amazon.

Link-local konektivitas

Agen terhubung ke GuardDuty backend melalui alamat link-lokal, di. `guardduty-data-v2.`*`us-east-1`*`.amazonaws.com` Link-localkonektivitas tidak menggunakan DNS pribadi. Wilayah AWS (*`us-east-1`*) berubah berdasarkan Wilayah Anda.

Konektivitas titik akhir Amazon VPC

Agen terhubung ke GuardDuty backend melalui titik akhir VPC Amazon. Ini menyelesaikan dan menghubungkan ke nama DNS pribadi titik akhir. Untuk titik akhir non-FIPS, ini adalah. `guardduty-data.`*`us-east-1`*`.amazonaws.com` Wilayah AWS (*`us-east-1`*) berubah berdasarkan Wilayah Anda.

Sumber daya harus memiliki jalur jaringan yang valid ke titik akhir VPC `guardduty-data` Amazon yang aktif. GuardDuty memilih subnet berdasarkan ketersediaan IP, jadi untuk topologi jaringan tingkat lanjut, validasi konektivitas itu dimungkinkan.

Prasyarat

Untuk prasyarat, lihat. Prasyarat untuk mengaktifkan Pemantauan Runtime

Pertimbangan-pertimbangan

- Semua VPC — Dengan konfigurasi agen otomatis, GuardDuty atur konektivitas di semua VPC Anda, termasuk VPC terpusat dan spoke. Untuk informasi selengkapnya tentang VPC terpusat, lihat Endpoint VPC Antarmuka di AWS Whitepaper - Membangun Infrastruktur Jaringan yang Dapat Diskalakan dan Aman. Multi-VPC AWS
- VPC Bersama — Jika Anda menggunakan VPC bersama, gunakan VPC bersama GuardDuty tersebut untuk menerima peristiwa runtime dari sumber daya Anda setelah prasyarat terpenuhi. Lihat Menggunakan VPC bersama dengan Runtime Monitoring.

Topik terkait

- Menyebarkan agen keamanan ke Amazon EC2
- Menyebarkan agen keamanan ke Amazon EKS
- Menyebarkan agen keamanan ke Amazon ECS di Fargate
- Meninjau statistik cakupan runtime dan masalah pemecahan masalah

Melacak cakupan Pemantauan Runtime

Setelah mengaktifkan Runtime Monitoring dan menginstal agen GuardDuty keamanan di akun mandiri atau beberapa akun anggota, Anda dapat mengambil langkah-langkah berikut untuk memastikan bahwa pengaturan rencana perlindungan berfungsi seperti yang diharapkan, dan memantau berapa banyak memori dan CPU yang digunakan agen GuardDuty keamanan.

Menilai cakupan runtime

GuardDuty merekomendasikan Anda untuk terus menilai status cakupan sumber daya tempat Anda menggunakan agen keamanan. Status cakupan bisa sehat atau tidak sehat. Status cakupan Sehat menunjukkan GuardDuty bahwa menerima peristiwa runtime dari sumber daya yang sesuai ketika ada aktivitas tingkat sistem operasi.

Ketika status cakupan menjadi Sehat untuk sumber daya, GuardDuty dapat menerima peristiwa runtime dan menganalisisnya untuk deteksi ancaman. Saat GuardDuty mendeteksi potensi ancaman keamanan dalam tugas atau aplikasi yang berjalan di beban kerja dan instance container Anda, hasilkan. GuardDuty GuardDuty Jenis penemuan Runtime Monitoring

Anda juga dapat mengonfigurasi Amazon EventBridge (EventBridge) untuk menerima pemberitahuan ketika status cakupan berubah dari Tidak Sehat menjadi Sehat dan sebaliknya. Untuk informasi selengkapnya, lihat Meninjau statistik cakupan runtime dan masalah pemecahan masalah.

Mengatur CPU dan pemantauan memori untuk agen GuardDuty keamanan

Setelah Anda menilai bahwa status cakupan ditampilkan sebagai Sehat, Anda dapat mengevaluasi kinerja agen keamanan untuk jenis sumber daya Anda. Untuk kluster Amazon EKS yang memiliki rilis agen keamanan v1.5 atau lebih tinggi, GuardDuty mendukung konfigurasi parameter agen keamanan (add-on). Untuk informasi selengkapnya, lihat Menyiapkan CPU dan pemantauan memori.

Bagaimana cara kerja uji coba gratis 30 hari di Runtime Monitoring

Masa uji coba gratis 30 hari bekerja secara berbeda untuk GuardDuty akun baru dan akun yang sudah ada yang telah mengaktifkan EKS Runtime Monitoring sebelum kemampuan Runtime Monitoring diperluas ke instans Amazon EC2 dan (AWS Fargate hanya Amazon ECS).

Saya menggunakan masa GuardDuty percobaan atau saya tidak pernah mengaktifkan EKS Runtime Monitoring

Daftar berikut menjelaskan cara kerja periode uji coba gratis 30 hari jika Anda menggunakan periode uji coba GuardDuty 30 hari atau belum pernah mengaktifkan EKS Runtime Monitoring:

- Saat Anda mengaktifkan GuardDuty untuk pertama kalinya, Runtime Monitoring dan EKS Runtime Monitoring tidak akan diaktifkan secara default.

  Saat Anda mengaktifkan Runtime Monitoring untuk akun atau organisasi Anda, pastikan juga mengonfigurasi agen GuardDuty keamanan untuk sumber daya yang ingin Anda pantau untuk deteksi ancaman. Misalnya, jika Anda ingin menggunakan Runtime Monitoring untuk instans Amazon EC2, setelah mengaktifkan Runtime Monitoring, Anda juga harus mengonfigurasi agen keamanan untuk Amazon EC2. Anda dapat memilih untuk melakukan ini baik secara manual atau otomatis melalui GuardDuty.
- Paket perlindungan Runtime Monitoring diaktifkan di tingkat akun. Periode uji coba gratis 30 hari bekerja di tingkat sumber daya. Setelah agen GuardDuty keamanan diterapkan ke jenis sumber daya tertentu, uji coba gratis 30 hari dimulai saat GuardDuty menerima peristiwa runtime pertama yang terkait dengan jenis sumber daya ini. Misalnya, Anda telah menerapkan GuardDuty agen di tingkat sumber daya (untuk instans Amazon EC2, cluster Amazon ECS, dan kluster Amazon EKS). Saat GuardDuty menerima acara runtime pertama untuk instans Amazon EC2, uji coba gratis 30 hari hanya akan dimulai untuk Amazon EC2.
- Bila Anda hanya ingin mengaktifkan EKS Runtime Monitoring — Saat Anda mengaktifkan GuardDuty untuk pertama kalinya, EKS Runtime Monitoring tidak diaktifkan secara default (setelah rilis Runtime Monitoring). Anda harus mengaktifkan EKS Runtime Monitoring. Untuk menggunakannya secara optimal, pastikan Anda mengelola agen GuardDuty keamanan secara manual atau mengaktifkan konfigurasi agen otomatis sehingga GuardDuty mengelola agen atas nama Anda. Periode uji coba gratis 30 hari untuk EKS Runtime Monitoring dimulai saat GuardDuty menerima acara runtime pertamanya untuk sumber daya Amazon EKS.

Saya mengaktifkan EKS Runtime Monitoring sebelum peluncuran Runtime Monitoring

Gunakan bagian ini hanya ketika EKS Runtime Monitoring diaktifkan untuk Anda Akun AWS, dan sekarang Anda ingin bermigrasi ke Runtime Monitoring.

Daftar berikut mencakup skenario yang mungkin berlaku untuk kasus penggunaan Anda mengaktifkan Runtime Monitoring:

- Untuk GuardDuty akun yang sudah ada yang mengaktifkan paket perlindungan Pemantauan Runtime EKS dan menggunakan pengalaman GuardDuty konsol untuk menggunakan paket perlindungan ini — Dengan pengumuman Runtime Monitoring, pengalaman konsol Pemantauan Runtime EKS kini telah dikonsolidasikan ke dalam Runtime Monitoring. Konfigurasi Anda yang ada untuk EKS Runtime Monitoring tetap sama. Anda dapat terus menggunakan API/CLI dukungan untuk melakukan operasi yang terkait dengan EKS Runtime Monitoring.
- Untuk menggunakan EKS Runtime Monitoring sebagai bagian dari Runtime Monitoring, Anda perlu mengonfigurasi Runtime Monitoring untuk akun atau organisasi Anda. Untuk menjaga konfigurasi yang sama untuk Runtime Monitoring, lihatBermigrasi dari Pemantauan Runtime EKS ke Pemantauan Runtime. Namun, ini tidak akan memengaruhi uji coba gratis 30 hari Anda untuk sumber daya Amazon EKS.
- Paket perlindungan Runtime Monitoring diaktifkan pada tingkat akun per Wilayah. Setelah agen GuardDuty keamanan diterapkan ke salah satu jenis sumber daya yang ditentukan (instans Amazon EC2 dan kluster Amazon ECS), uji coba gratis 30 hari dimulai GuardDuty saat menerima peristiwa runtime pertama yang terkait dengan sumber daya. Ada uji coba gratis 30 hari yang terkait dengan setiap jenis sumber daya.

  Misalnya, setelah mengaktifkan Runtime Monitoring, Anda memilih untuk menerapkan GuardDuty agen hanya di instans Amazon EC2, uji coba gratis 30 hari untuk sumber daya ini hanya akan dimulai saat GuardDuty menerima peristiwa runtime pertamanya untuk instans Amazon EC2. Kemudian, saat Anda menerapkan GuardDuty agen untuk Fargate (hanya Amazon ECS), uji coba gratis 30 hari untuk sumber daya ini hanya akan dimulai GuardDuty saat menerima acara runtime pertamanya untuk cluster Amazon ECS. Mengingat Anda sudah mengaktifkan EKS Runtime Monitoring untuk akun Anda, GuardDuty tidak mengatur ulang uji coba gratis 30 hari untuk sumber daya Amazon EKS.

Prasyarat untuk mengaktifkan Pemantauan Runtime

Untuk mengaktifkan Runtime Monitoring dan mengelola agen GuardDuty keamanan, Anda harus memenuhi prasyarat untuk setiap jenis sumber daya yang ingin Anda pantau untuk deteksi ancaman. Setiap jenis sumber daya memiliki prasyarat yang berbeda. Misalnya, GuardDuty mendukung distribusi OS yang berbeda berdasarkan jenis sumber daya.

Saat Anda hanya ingin memantau sumber daya Amazon EC2, Anda akan mengikuti prasyarat untuk instans Amazon EC2. Jika di lain waktu, Anda memilih untuk memantau sumber daya Amazon EKS, Anda harus mengikuti prasyarat khusus untuk kluster Amazon EKS.

Bagian berikut mencakup prasyarat berdasarkan jenis sumber daya.

Daftar Isi

- Prasyarat untuk dukungan instans Amazon EC2
- Prasyarat untuk dukungan Bottlerocket ECS-EC2
- Prasyarat untuk AWS Fargate (Hanya Amazon ECS) dukungan
- Prasyarat untuk dukungan klaster Amazon EKS
- Arsitektur CPU, sistem operasi, dan versi kernel yang didukung

Prasyarat untuk dukungan instans Amazon EC2

Bagian ini mencakup prasyarat untuk memantau perilaku runtime instans Amazon EC2 Anda. Setelah prasyarat ini terpenuhi, lihat. Mengaktifkan GuardDuty Runtime Monitoring

Topik

- Jadikan instans EC2 SSM dikelola (hanya untuk konfigurasi agen otomatis)
- Validasi persyaratan arsitektur
- Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun
- Saat menggunakan konfigurasi agen otomatis
- CPU dan batas memori untuk GuardDuty agen
- Langkah berikutnya

Jadikan instans EC2 SSM dikelola (hanya untuk konfigurasi agen otomatis)

GuardDuty menggunakan AWS Systems Manager (SSM) untuk secara otomatis menyebarkan, menginstal, dan mengelola agen keamanan pada instans Anda. Jika Anda berencana untuk menginstal dan mengelola GuardDuty agen secara manual, SSM tidak diperlukan.

Untuk mengelola instans Amazon EC2 dengan Systems Manager, lihat Menyiapkan Systems Manager untuk instans Amazon EC2 di Panduan Pengguna.AWS Systems Manager

Validasi persyaratan arsitektur

Arsitektur distribusi OS Anda dapat memengaruhi perilaku agen GuardDuty keamanan. Anda harus memenuhi persyaratan berikut sebelum menggunakan Runtime Monitoring untuk instans Amazon EC2:

Untuk arsitektur CPU terverifikasi, distribusi OS, dan versi kernel, lihat. Arsitektur CPU, sistem operasi, dan versi kernel yang didukung

- Persyaratan tambahan - Hanya jika Anda memiliki Amazon ECS/Amazon EC2

  Untuk Amazon ECS/Amazon EC2, kami menyarankan Anda menggunakan ECS-optimized AMI Amazon terbaru (tertanggal 29 September 2023 atau lebih baru), atau gunakan agen Amazon ECS versi v1.77.0.

Melihat dan memperbarui nilai **RLIMIT_MEMLOCK**

Ketika `RLIMIT_MEMLOCK` batas sistem Anda ditetapkan terlalu rendah, agen GuardDuty keamanan mungkin tidak berfungsi seperti yang dirancang. GuardDuty merekomendasikan bahwa batas keras dan lunak harus setidaknya 32 MB. Jika Anda tidak memperbarui batas, tidak GuardDuty akan dapat memantau peristiwa runtime untuk sumber daya Anda. Ketika `RLIMIT_MEMLOCK` berada di atas batas minimum yang dinyatakan, itu menjadi opsional bagi Anda untuk memperbarui batas ini.

Anda dapat mengubah `RLIMIT_MEMLOCK` nilai default baik sebelum atau setelah menginstal agen GuardDuty keamanan.

Untuk melihat nilai **RLIMIT_MEMLOCK**

1. Jalankan `ps aux | grep guardduty`. Ini akan menampilkan ID proses (`pid`).
2. Salin ID proses (`pid`) dari output dari perintah sebelumnya.

3. Jalankan `grep "Max locked memory" /proc/pid/limits` setelah mengganti `pid` dengan ID proses yang disalin dari langkah sebelumnya.

   Ini akan menampilkan memori terkunci maksimum untuk menjalankan agen GuardDuty keamanan.

Untuk memperbarui nilai **`RLIMIT_MEMLOCK`**

1. Jika `/etc/systemd/system.conf.d/NUMBER-limits.conf` file ada, maka komentari baris `DefaultLimitMEMLOCK` dari file ini. File ini menetapkan default `RLIMIT_MEMLOCK` dengan prioritas tinggi, yang menimpa pengaturan Anda dalam `/etc/systemd/system.conf` file.
2. Buka `/etc/systemd/system.conf` file dan hapus komentar pada baris yang ada`#DefaultLimitMEMLOCK=`.
3. Perbarui nilai default dengan memberikan `RLIMIT_MEMLOCK` batas keras dan lunak setidaknya 32MB. Pembaruan akan terlihat seperti ini:`DefaultLimitMEMLOCK=32M:32M`. Formatnya adalah `soft-limit:hard-limit`.
4. Jalankan `sudo reboot`.

Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun

Jika Anda telah menyiapkan kebijakan kontrol layanan (SCP) untuk mengelola izin di organisasi Anda, validasi bahwa batas izin memungkinkan tindakan tersebut. `guardduty:SendSecurityTelemetry` GuardDuty memerlukan izin ini untuk mendukung Runtime Monitoring di berbagai jenis sumber daya.

Jika akun Anda adalah akun anggota, hubungi administrator yang didelegasikan terkait. Untuk informasi tentang mengelola SCP untuk organisasi Anda, lihat Kebijakan kontrol layanan (SCP).

Saat menggunakan konfigurasi agen otomatis

UntukKonfigurasi agen otomatis (disarankan), Anda Akun AWS harus memenuhi prasyarat berikut:

- Saat menggunakan tag inklusi dengan konfigurasi agen otomatis, GuardDuty untuk membuat asosiasi SSM untuk instance baru, pastikan instans baru dikelola SSM dan muncul di bawah Fleet Manager di https://console.aws.amazon.com/systems-manager/konsol.
- Saat menggunakan tag pengecualian dengan konfigurasi agen otomatis:

- Tambahkan `false` tag`GuardDutyManaged`: sebelum mengonfigurasi agen GuardDuty otomatis untuk akun Anda.

  Pastikan Anda menambahkan tag pengecualian ke instans Amazon EC2 sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2, instans EC2 apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen otomatis. GuardDuty
- Aktifkan Izinkan tag dalam pengaturan metadata untuk instance Anda. Pengaturan ini diperlukan karena GuardDuty perlu membaca tag pengecualian dari layanan metadata instance (IMDS) untuk menentukan apakah harus mengecualikan instance dari instalasi agen. Untuk informasi selengkapnya, lihat Mengaktifkan akses ke tag dalam metadata instans di Panduan Pengguna Amazon EC2.

CPU dan batas memori untuk GuardDuty agen

Batas CPU

GuardDuty membatasi agen keamanan hingga 10 persen dari total kapasitas vCPU pada instance. Misalnya, pada instance dengan 4 inti vCPU, agen dapat menggunakan paling banyak 0,4 vCPU.

Batas memori

Dari memori yang terkait dengan instans Amazon EC2 Anda, ada memori terbatas yang dapat digunakan agen GuardDuty keamanan.

Tabel berikut menunjukkan batas memori.

Memori instans Amazon EC2	Memori maksimum untuk GuardDuty agen
Kurang dari 8 GB	128 MB
8 GB hingga kurang dari 32 GB	270 MB
Lebih dari atau sama dengan 32 GB	1 GB

Langkah berikutnya

Langkah selanjutnya adalah mengkonfigurasi Runtime Monitoring dan juga mengelola agen keamanan (secara otomatis atau manual).

Prasyarat untuk dukungan Bottlerocket ECS-EC2

> **Important**
>
> Bagian ini hanya berlaku untuk versi ECS-optimized *v1.62.1*AMI Bottlerocket ke atas, termasuk varian berikut:
>
> - `bottlerocket-aws-ecs-2-x86_64` / `bottlerocket-aws-ecs-2-aarch64`
> - `bottlerocket-aws-ecs-3-x86_64` / `bottlerocket-aws-ecs-3-aarch64`
> - `bottlerocket-aws-ecs-2-nvidia` / `bottlerocket-aws-ecs-2-nvidia-fips`
> - `bottlerocket-aws-ecs-3-nvidia` / `bottlerocket-aws-ecs-3-nvidia-fips`

Runtime Monitoring memperluas GuardDuty deteksi ancaman ke instans Amazon EC2 Bottlerocket Anda di cluster Amazon ECS, menggunakan agen keamanan yang berjalan sebagai wadah host agar sesuai dengan desain yang dioptimalkan untuk wadah Bottlerocket. Untuk mengaktifkannya, lengkapi prasyarat di bagian ini. Setelah prasyarat ini terpenuhi, lihat. Mengaktifkan GuardDuty Runtime Monitoring

Untuk informasi selengkapnya tentang persyaratan dan instruksi, lihatMengelola agen GuardDuty keamanan di Bottlerocket (Amazon ECS di Amazon EC2).

Topik

- Jadikan instans EC2 SSM dikelola dan konfigurasikan izin instans
- Memvalidasi persyaratan arsitektur
- Persyaratan konektivitas jaringan
- Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun
- Saat menggunakan konfigurasi agen otomatis
- CPU dan batas memori untuk GuardDuty agen
- Langkah berikutnya

Jadikan instans EC2 SSM dikelola dan konfigurasikan izin instans

GuardDuty menggunakan AWS Systems Manager (SSM) untuk menyebarkan, menginstal, dan mengelola agen keamanan pada instance Bottlerocket Anda, berjalan melalui agen SSM di wadah kontrol Bottlerocket.

Dalam kebanyakan kasus, izin yang sudah dimiliki instans Anda untuk Bottlerocket juga mencakup. GuardDuty Tidak diperlukan kebijakan tambahan. `AmazonEC2ContainerRegistryReadOnly`Kebijakan yang digunakan Bottlerocket untuk menarik kontrol dan gambar kontainer admin juga memenuhi GuardDuty persyaratan untuk menarik gambar wadah agen. Untuk informasi lebih lanjut, lihat Bottlerocket README.

Profil instans harus menyertakan kebijakan terkelola berikut:

- `AmazonSSMManagedInstanceCore`- Diperlukan untuk wadah kontrol Bottlerocket untuk menjalankan agen SSM. Untuk mengelola instans Amazon EC2 dengan Systems Manager, lihat Menyiapkan Systems Manager untuk instans Amazon EC2 di Panduan Pengguna.AWS Systems Manager
- `AmazonEC2ContainerRegistryReadOnly`- Diperlukan untuk menarik gambar wadah GuardDuty agen dari Amazon ECR. Minimal, izin berikut diperlukan:

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

Untuk lebih membatasi izin Amazon ECR, Anda dapat menambahkan URI repositori Amazon ECR yang menampung GuardDuty agen keamanan untuk Amazon EC2 Bottlerocket. ECS-Amazon Untuk informasi selengkapnya, lihat Repositori ECR untuk GuardDuty agen di Bottlerocket ECS-EC2.

Memvalidasi persyaratan arsitektur

Arsitektur instance Anda menentukan bagaimana agen GuardDuty keamanan berperilaku. Bottlerocket ECS-2 dan ECS-3 varian memenuhi persyaratan ini di luar kotak. Konfirmasikan hal berikut sebelum mengaktifkan Runtime Monitoring:

- Dukungan kernel meliputieBPF,`Tracepoints`, dan`Kprobe`. Varian bottlerocket menggunakan kernel `6.1` dan ECS-2 ECS-3 varian menggunakan kernel. `6.12` Kedua versi memenuhi persyaratan kernel untuk Runtime Monitoring. Opsi `CONFIG_DEBUG_INFO_BTF=y` kernel diaktifkan secara default di ECS-2 Bottlerocket dan kernel. ECS-3
- Untuk arsitektur CPU, Runtime Monitoring mendukung AMD64 (`x86_64`) dan ARM64 (). `aarch64`

Persyaratan konektivitas jaringan

GuardDuty meng-host agen keamanannya sebagai gambar kontainer di Amazon ECR, jadi instans Anda memerlukan konektivitas jaringan ke Amazon ECR untuk menariknya. Bergantung pada konfigurasi jaringan Anda, pilih salah satu opsi berikut:

Opsi 1 - Menggunakan akses jaringan publik (jika tersedia)

Jika instans Bottlerocket Anda berjalan di subnet dengan akses internet keluar, tidak diperlukan konfigurasi jaringan tambahan.

Opsi 2 - Menggunakan titik akhir Amazon VPC (untuk subnet pribadi)

Untuk instance Bottlerocket di subnet pribadi, titik akhir VPC menyediakan konektivitas yang dibutuhkan agen. Konfigurasikan titik akhir untuk Amazon ECR, Amazon S3, dan Systems Manager sehingga instance dapat menarik image agen dan berkomunikasi dengan Systems Manager untuk penerapan.

Untuk informasi selengkapnya tentang mengonfigurasi titik akhir VPC, lihat Membuat titik akhir VPC untuk Amazon ECR di Panduan Pengguna Amazon Elastic Container Registry dan Membuat titik akhir VPC di Panduan Pengguna.AWS Systems Manager

Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun

Jika Anda telah menyiapkan kebijakan kontrol layanan (SCP) untuk mengelola izin di organisasi Anda, validasi bahwa batas izin memungkinkan tindakan tersebut. `guardduty:SendSecurityTelemetry` GuardDuty memerlukan izin ini untuk mendukung Runtime Monitoring di berbagai jenis sumber daya.

Jika akun Anda adalah akun anggota, hubungi administrator yang didelegasikan terkait. Untuk informasi tentang mengelola SCP untuk organisasi Anda, lihat Kebijakan kontrol layanan (SCP).

Saat menggunakan konfigurasi agen otomatis

Untuk menggunakan konfigurasi agen otomatis, Anda Akun AWS harus memenuhi prasyarat berikut:

- Saat menggunakan tag inklusi dengan konfigurasi agen otomatis, GuardDuty untuk membuat asosiasi SSM untuk instance baru, pastikan instans baru dikelola SSM dan muncul di bawah Fleet Manager di https://console.aws.amazon.com/systems-manager/konsol.
- Saat menggunakan tag pengecualian dengan konfigurasi agen otomatis:
  - Tambahkan `false` tag`GuardDutyManaged`: ke instans Amazon EC2 sebelum Anda meluncurkannya, dan sebelum Anda mengonfigurasi agen GuardDuty otomatis untuk akun Anda. Setelah konfigurasi agen otomatis diaktifkan, setiap instance yang diluncurkan tanpa tag pengecualian akan tercakup secara otomatis.
  - Aktifkan Izinkan tag dalam pengaturan metadata untuk instance Anda. Pengaturan ini diperlukan karena GuardDuty perlu membaca tag pengecualian dari layanan metadata instance (IMDS) untuk menentukan apakah harus mengecualikan instance dari instalasi agen. Untuk informasi selengkapnya, lihat Mengaktifkan akses ke tag dalam metadata instans di Panduan Pengguna Amazon EC2.

CPU dan batas memori untuk GuardDuty agen

Batas CPU

GuardDuty membatasi agen keamanan hingga 10 persen dari total kapasitas vCPU pada instance. Misalnya, pada instance dengan 4 inti vCPU, agen dapat menggunakan paling banyak 0,4 vCPU.

Batas memori

Dari memori yang terkait dengan instans Amazon EC2 Anda, ada batasan pada memori yang dapat digunakan agen GuardDuty keamanan.

Tabel berikut menunjukkan batas memori.

Memori instans Amazon EC2	Memori maksimum untuk GuardDuty agen
Kurang dari 8 GB	128 MB
8 GB hingga kurang dari 32 GB	270 MB

Memori instans Amazon EC2	Memori maksimum untuk GuardDuty agen
Lebih dari atau sama dengan 32 GB	1 GB

Langkah berikutnya

Langkah Anda selanjutnya adalah mengonfigurasi Runtime Monitoring dan mengelola agen keamanan secara otomatis.

Prasyarat untuk AWS Fargate (Hanya Amazon ECS) dukungan

Bagian ini mencakup prasyarat untuk memantau perilaku runtime sumber daya ECS Anda. Fargate-Amazon Setelah prasyarat ini terpenuhi, lihat. Mengaktifkan GuardDuty Runtime Monitoring

Topik

- Memvalidasi persyaratan arsitektur
- Prasyarat untuk akses gambar kontainer
- Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun
- Memvalidasi izin peran dan batas izin kebijakan
- Batas CPU dan memori

Memvalidasi persyaratan arsitektur

Platform yang Anda gunakan dapat memengaruhi cara agen GuardDuty keamanan mendukung GuardDuty dalam menerima peristiwa runtime dari kluster Amazon ECS Anda. Anda harus memvalidasi bahwa Anda menggunakan salah satu platform terverifikasi.

Pertimbangan awal:

AWS Fargate Platform untuk cluster Amazon ECS Anda harus Linux. Versi platform yang sesuai harus setidaknya`1.4.0`, atau`LATEST`. Untuk informasi selengkapnya tentang versi platform, lihat versi platform Linux di Panduan Pengembang Layanan Amazon Elastic Container.

Versi platform Windows belum didukung.

Untuk arsitektur CPU terverifikasi, distribusi OS, dan versi kernel, lihat. Arsitektur CPU, sistem operasi, dan versi kernel yang didukung

Prasyarat untuk akses gambar kontainer

Prasyarat berikut membantu Anda mengakses gambar GuardDuty kontainer sespan dari repositori Amazon ECR.

Persyaratan izin

Peran eksekusi tugas memerlukan izin Amazon Elastic Container Registry (Amazon ECR) tertentu untuk mengunduh GuardDuty gambar kontainer agen keamanan:

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

Untuk lebih membatasi izin Amazon ECR, Anda dapat menambahkan URI repositori Amazon ECR yang menampung GuardDuty agen keamanan untuk (AWS Fargate hanya Amazon ECS). Untuk informasi selengkapnya, lihat Agen hosting repositori Amazon ECR GuardDuty.

Anda dapat menggunakan kebijakan AmazonECSTaskExecutionRolePolicyterkelola atau menambahkan izin di atas ke `TaskExecutionRole` kebijakan Anda.

Konfigurasi definisi tugas

Saat membuat atau memperbarui layanan Amazon ECS, Anda perlu memberikan informasi subnet dalam definisi tugas Anda:

Menjalankan UpdateServiceAPI CreateServicedan API di Amazon Elastic Container Service API Reference mengharuskan Anda meneruskan informasi subnet. Untuk informasi selengkapnya, lihat definisi tugas Amazon ECS di Panduan Pengembang Layanan Kontainer Elastis Amazon.

Persyaratan konektivitas jaringan

Anda harus memastikan konektivitas jaringan untuk mengunduh gambar GuardDuty kontainer dari Amazon ECR. Persyaratan ini khusus untuk GuardDuty karena menggunakan Amazon ECR untuk meng-host agen keamanannya. Bergantung pada konfigurasi jaringan Anda, Anda perlu menerapkan salah satu opsi berikut:

Opsi 1 - Menggunakan akses jaringan publik (jika tersedia)

Jika tugas Fargate Anda berjalan di subnet dengan akses internet keluar, tidak diperlukan konfigurasi jaringan tambahan.

Opsi 2 - Menggunakan titik akhir Amazon VPC (untuk subnet pribadi)

Jika tugas Fargate Anda berjalan di subnet pribadi tanpa akses internet, Anda harus mengonfigurasi titik akhir VPC untuk ECR guna memastikan bahwa URI repositori ECR yang menampung agen keamanan dapat diakses jaringan. GuardDuty Tanpa titik akhir ini, tugas dalam subnet pribadi tidak dapat mengunduh gambar GuardDuty kontainer.

Untuk petunjuk penyiapan titik akhir VPC, lihat Membuat titik akhir VPC untuk Amazon ECR di Panduan Pengguna Amazon Elastic Container Registry.

Untuk informasi tentang mengaktifkan Fargate mengunduh GuardDuty penampung, lihat Menggunakan gambar Amazon ECR dengan Amazon ECS di Panduan Pengguna Amazon Elastic Container Registry.

Konfigurasi grup keamanan

Gambar GuardDuty kontainer ada di Amazon ECR dan memerlukan akses Amazon S3. Persyaratan ini khusus untuk mengunduh gambar kontainer dari Amazon ECR. Untuk tugas dengan akses jaringan terbatas, Anda harus mengonfigurasi grup keamanan Anda untuk mengizinkan akses ke S3.

Tambahkan aturan keluar di grup keamanan Anda yang memungkinkan lalu lintas ke daftar awalan terkelola S3 (`pl-xxxxxxxx`) pada port 443. Untuk menambahkan aturan keluar, lihat Mengonfigurasi aturan grup keamanan di Panduan Pengguna Amazon VPC.

Untuk melihat daftar awalan AWS-managed di konsol atau mendeskripsikannya dengan menggunakan AWS Command Line Interface (AWS CLI), lihat daftar awalan AWS-managed di Panduan Pengguna Amazon VPC.

Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun

Bagian ini menjelaskan cara memvalidasi setelan kebijakan kontrol layanan (SCP) Anda untuk memastikan Runtime Monitoring berfungsi seperti yang diharapkan di seluruh organisasi Anda.

Jika Anda telah menyiapkan satu atau beberapa kebijakan kontrol layanan untuk mengelola izin di organisasi, Anda harus memvalidasi bahwa kebijakan tersebut tidak menolak tindakan

tersebut`guardduty:SendSecurityTelemetry`. Untuk informasi tentang cara kerja SCP, lihat evaluasi SCP di AWS Organizations Panduan Pengguna.

Jika akun Anda adalah akun anggota, hubungi administrator yang didelegasikan terkait. Untuk informasi tentang mengelola SCP untuk organisasi Anda, lihat Kebijakan kontrol layanan (SCP) di AWS Organizations Panduan Pengguna.

Lakukan langkah-langkah berikut untuk semua SCP yang telah Anda siapkan di lingkungan multi-akun Anda:

Untuk memvalidasi **`tugas jaga:`** tidak ditolak di SendSecurityTelemetry SCP

1. Masuk ke konsol Organizations di https://console.aws.amazon.com/organizations/. Anda harus masuk sebagai peran IAM, atau masuk sebagai pengguna root (tidak disarankan) di akun manajemen organisasi.
2. Pada panel navigasi sebelah kiri, pilih Kebijakan. Kemudian, di bawah Jenis kebijakan yang didukung, pilih Kebijakan kontrol layanan.
3. Pada halaman Kebijakan kontrol layanan, pilih nama kebijakan yang ingin Anda validasi.
4. Pada halaman detail kebijakan, lihat Konten kebijakan ini. Pastikan bahwa itu tidak menyangkal `guardduty:SendSecurityTelemetry` tindakan.

   Kebijakan SCP berikut adalah contoh untuk tidak menyangkal tindakan: `guardduty:SendSecurityTelemetry`

   JSON

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

Jika kebijakan Anda menolak tindakan ini, Anda harus memperbarui kebijakan tersebut. Untuk informasi selengkapnya, lihat Memperbarui kebijakan kontrol layanan (SCP) di Panduan AWS Organizations Pengguna.

Memvalidasi izin peran dan batas izin kebijakan

Gunakan langkah-langkah berikut untuk memvalidasi bahwa batas izin yang terkait dengan peran dan kebijakannya tidak membatasi `guardduty:SendSecurityTelemetry` tindakan.

Untuk melihat batas izin untuk peran dan kebijakannya

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi kiri, di bawah Manajemen akses, pilih Peran.
3. Pada halaman Peran, pilih peran *`TaskExecutionRole`* yang mungkin telah Anda buat.
4. Pada halaman peran yang dipilih, di bawah tab Izin, perluas nama kebijakan yang terkait dengan peran ini. Kemudian, validasi bahwa kebijakan ini tidak membatasi`guardduty:SendSecurityTelemetry`.
5. Jika batas Izin ditetapkan, maka perluas bagian ini. Kemudian, perluas setiap kebijakan untuk meninjau bahwa itu tidak membatasi `guardduty:SendSecurityTelemetry` tindakan. Kebijakan harus tampak mirip dengan iniExample SCP policy.

   Sesuai kebutuhan, lakukan salah satu tindakan berikut:

   - Untuk mengubah kebijakan, pilih Edit. Pada halaman Ubah izin untuk kebijakan ini, perbarui kebijakan di editor Kebijakan. Pastikan bahwa skema JSON tetap valid. Lalu, pilih Selanjutnya. Kemudian, Anda dapat meninjau dan menyimpan perubahan.
   - Untuk mengubah batas izin ini dan memilih batas lain, pilih Ubah batas.
   - Untuk menghapus batas izin ini, pilih Hapus batas.

   Untuk informasi tentang mengelola kebijakan, lihat Kebijakan dan izin AWS Identity and Access Management di Panduan Pengguna IAM.

Batas CPU dan memori

Dalam definisi tugas Fargate, Anda harus menentukan CPU dan nilai memori di tingkat tugas. Tabel berikut menunjukkan kombinasi yang valid dari CPU tingkat tugas dan nilai memori, dan batas memori maksimum agen GuardDuty keamanan yang sesuai untuk wadah. GuardDuty

Nilai CPU	Nilai memori	GuardDuty batas memori maksimum agen
256 (.25 vCPU)	512 MiB, 1 GB, 2GB	128 MB
512 (.5 vCPU)	1 GB, 2 GB, 3 GB, 4 GB	
1024 (1 vCPU)	2 GB, 3 GB, 4 GB	
	5 GB, 6 GB, 7 GB, 8 GB	
2048 (2 vCPU)	Antara 4 GB dan 16 GB dalam peningkatan 1 GB	
4096 (4 vCPU)	Antara 8 GB dan 20 GB dalam peningkatan 1 GB	
8192 (8 vCPU)	Antara 16 GB dan 28 GB dalam peningkatan 4 GB	270 MB
	Antara 32 GB dan 60 GB dalam peningkatan 4 GB	512 MB
16384 (16 vCPU)	Antara 32 GB dan 120 GB dalam peningkatan 8 GB	1 GB

Setelah mengaktifkan Runtime Monitoring dan menilai bahwa status cakupan klaster Anda Sehat, Anda dapat menyiapkan dan melihat metrik wawasan Container. Untuk informasi selengkapnya, lihat Menyiapkan pemantauan di Amazon ECS cluster.

Langkah selanjutnya adalah mengkonfigurasi Runtime Monitoring dan juga mengkonfigurasi agen keamanan.

Prasyarat untuk dukungan klaster Amazon EKS

Bagian ini mencakup prasyarat untuk memantau perilaku runtime sumber daya Amazon EKS Anda. Prasyarat ini sangat penting bagi GuardDuty agen untuk berfungsi seperti yang diharapkan. Setelah prasyarat ini terpenuhi, lihat Mengaktifkan GuardDuty Runtime Monitoring untuk mulai memantau sumber daya Anda.

Dukungan untuk fitur Amazon EKS

Runtime Monitoring mendukung klaster Amazon EKS yang berjalan di instans Amazon EC2 dan Mode Otomatis Amazon EKS.

Runtime Monitoring tidak mendukung kluster Amazon EKS dengan Amazon EKS Hybrid Nodes, dan yang berjalan. AWS Fargate

Untuk informasi tentang fitur Amazon EKS ini, lihat Apa itu Amazon EKS? di Panduan Pengguna Amazon EKS.

Memvalidasi persyaratan arsitektur

Platform yang Anda gunakan dapat memengaruhi cara agen GuardDuty keamanan mendukung GuardDuty dalam menerima peristiwa runtime dari kluster EKS Anda. Anda harus memvalidasi bahwa Anda menggunakan salah satu platform terverifikasi. Jika Anda mengelola GuardDuty agen secara manual, pastikan bahwa versi Kubernetes mendukung versi GuardDuty agen yang sedang digunakan.

Platform terverifikasi

Untuk arsitektur CPU terverifikasi, distribusi OS, dan versi kernel, lihat. Arsitektur CPU, sistem operasi, dan versi kernel yang didukung

Saat ini, dengan versi kernel `5.4` di ARM64 (`aarch64`), tidak GuardDuty dapat menghasilkan GuardDuty Jenis penemuan Runtime Monitoring yang terkait dengan. Acara Sistem Nama Domain (DNS)

Versi Kubernetes didukung oleh agen keamanan GuardDuty

Tabel berikut menunjukkan versi Kubernetes untuk kluster EKS Anda yang didukung oleh agen keamanan. GuardDuty

Amazon EKS versi agen GuardDuty keamanan add-on	Versi Kubernetes
v1.17.1 (terbaru - v1.17.1-eksbuild.2)	1,31 - 1,36
v1.16.0 (terbaru - v1.16.0-eksbuild.2)	1,28 - 1,36
v1.15.0 (terbaru - v1.15.0-eksbuild.2)	1,28 - 1,36
v1.12.2 (terbaru - v1.12.2-eksbuild.2)	1,28 - 1,36
v1.12.1 (terbaru - v1.12.1-eksbuild.4)	1,28 - 1,35
v1.11.0 (terbaru - v1.11.0-eksbuild.4)	1,28 - 1,34
v1.10.0 (terbaru - v1.10.0-eksbuild.2)	1,21 - 1,33
v1.9.0 (terbaru - v1.9.0-eksbuild.2) v1.8.1 (terbaru - v1.8.1-eksbuild.2)	1,21 - 1,32
v1.7.1 v1.7.0 v1.6.1	1,21 - 1,31
v1.6.0 v1.5.0 v1.4.1 v1.4.0 v1.3.1	1,21 - 1,29
v1.3.0 v1.2.0	1,21 - 1,28
v1.1.0	1,21 - 1,26

Amazon EKS versi agen GuardDuty keamanan add-on	Versi Kubernetes
v1.0.0	1,21 - 1,25

Beberapa versi agen GuardDuty keamanan akan mencapai akhir dukungan standar.

Untuk informasi tentang versi rilis agen, lihatGuardDuty versi agen keamanan untuk sumber daya Amazon EKS.

Batas CPU dan memori

Tabel berikut menunjukkan batas CPU dan memori untuk add-on Amazon EKS for GuardDuty (`aws-guardduty-agent`).

Parameter	Batas minimum	Batas maksimum
CPU	200m	1000m
Memori	257 Mi	1024 Mi

Saat Anda menggunakan add-on Amazon EKS versi 1.5.0 atau yang lebih baru, GuardDuty menyediakan kemampuan untuk mengonfigurasi skema add-on untuk nilai CPU dan memori Anda. Untuk informasi tentang rentang yang dapat dikonfigurasi, lihatParameter dan nilai yang dapat dikonfigurasi.

Setelah mengaktifkan EKS Runtime Monitoring dan menilai status cakupan klaster EKS Anda, Anda dapat mengatur dan melihat metrik wawasan container. Untuk informasi selengkapnya, lihat Menyiapkan CPU dan pemantauan memori.

Memvalidasi kebijakan kontrol layanan organisasi Anda

Jika Anda telah menyiapkan kebijakan kontrol layanan (SCP) untuk mengelola izin di organisasi Anda, validasi bahwa batas izin tidak membatasi. `guardduty:SendSecurityTelemetry` GuardDuty memerlukan izin ini untuk mendukung Runtime Monitoring di berbagai jenis sumber daya.

Jika akun Anda adalah akun anggota, hubungi administrator yang didelegasikan terkait. Untuk informasi tentang mengelola SCP untuk organisasi Anda, lihat Kebijakan kontrol layanan (SCP).

Arsitektur CPU, sistem operasi, dan versi kernel yang didukung

Bagian ini mengkonsolidasikan arsitektur CPU, distribusi OS, dan versi kernel yang telah diverifikasi untuk mendukung agen keamanan. GuardDuty Kecuali jenis sumber daya dipanggil secara terpisah, persyaratan ini berlaku untuk Pemantauan Waktu Proses untuk instans Amazon EC2, AWS Fargate (hanya Amazon ECS), dan kluster Amazon EKS.

Dukungan kernel meliputieBPF,`Tracepoints`, dan`Kprobe`. Untuk arsitektur CPU, Runtime Monitoring mendukung AMD64 (`x64`) dan ARM64 (Graviton2 dan di atasnya). [1]

Tabel berikut menunjukkan distribusi OS dan versi kernel yang telah diverifikasi untuk mendukung agen GuardDuty keamanan.

Distribusi OS [2]	Versi kernel [3]
Amazon Linux 2	5.4 [4], 5.10, 5.15 [4]
Amazon Linux 2023	5.4 [4], 5.10, 5.15 [4], 6.1, 6.5, 6.8, 6.12
Ubuntu 20.04, 22.04, 24.04, 26.04	5.4 [4], 5.10, 5.15 [4], 6.1, 6.5, 6.8, 6.13, 6.14, 6.15, 6.16, 6.17, 6.18, 7.0
Debian 11, 12, 13	5.4 [4], 5.10, 5.15 [4], 6.1, 6.5, 6.8, 6.12
RedHat 9.4, 10.2	5.14, 6.12
Fedora 34, 40, 41, 43, 44	5.11, 5.17, 6.8, 6.12, 7.1
CentOS Aliran 9, 10	5.14, 6.12
Oracle Linux 8.9, 9.3	5.15
Linux Berbatu 9.5, 10.1	5.14, 6.12
Alma Linux 9, 10	5.14, 6.12
SUSE Linux Server Perusahaan 16	6.12

Distribusi OS [2]	Versi kernel [3]
Bottlerocket	5.4 [4], 5.10, 5.15 [4], 6.1, 6.18

1. Runtime Monitoring tidak mendukung instance Graviton generasi pertama seperti tipe instans A1.
2. Support untuk berbagai sistem operasi - GuardDuty telah memverifikasi dukungan Runtime Monitoring untuk distribusi operasi yang tercantum dalam tabel sebelumnya. Sementara agen GuardDuty keamanan dapat berjalan pada sistem operasi yang tidak tercantum dalam tabel sebelumnya, GuardDuty tim tidak dapat menjamin nilai keamanan yang diharapkan.
3. Untuk versi kernel apa pun, Anda harus menyetel `CONFIG_DEBUG_INFO_BTF` flag ke y (artinya true). Ini diperlukan agar agen GuardDuty keamanan dapat berjalan seperti yang diharapkan.

   Untuk AWS Fargate (hanya Amazon ECS), opsi kernel ini dikelola oleh Fargate dan tidak memerlukan tindakan dari Anda.
4. Untuk kernel versi 5.10 dan sebelumnya, agen GuardDuty keamanan menggunakan memori terkunci di RAM (`RLIMIT_MEMLOCK`) berfungsi seperti yang diharapkan. Jika `RLIMIT_MEMLOCK` nilai sistem Anda disetel terlalu rendah, GuardDuty rekomendasikan pengaturan batas keras dan lunak setidaknya 32 MB. Untuk informasi tentang memverifikasi dan memodifikasi `RLIMIT_MEMLOCK` nilai default pada instans Amazon EC2, lihat. Melihat dan memperbarui nilai `RLIMIT_MEMLOCK`

Mengaktifkan GuardDuty Runtime Monitoring

Sebelum mengaktifkan Runtime Monitoring di akun Anda, pastikan bahwa jenis sumber daya yang ingin Anda pantau peristiwa runtime, mendukung persyaratan platform. Untuk informasi selengkapnya, lihat Prasyarat.

Jika Anda telah menggunakan EKS Runtime Monitoring sebelum peluncuran Runtime Monitoring, Anda dapat menggunakan API untuk memeriksa dan memperbarui konfigurasi yang ada untuk EKS Runtime Monitoring. Anda juga dapat memigrasikan konfigurasi yang ada dari EKS Runtime Monitoring ke Runtime Monitoring. Untuk informasi selengkapnya, lihat Bermigrasi dari Pemantauan Runtime EKS ke Pemantauan Runtime.

> **Note**
>
> Saat ini, dokumentasi ini menyediakan langkah-langkah untuk mengaktifkan Runtime Monitoring untuk akun dan organisasi Anda hanya berdasarkan konsol. Anda juga dapat mengaktifkan Runtime Monitoring dengan menggunakan API Actions atau AWS CLI for GuardDuty.

Anda dapat mengonfigurasi Runtime Monitoring dengan menggunakan langkah-langkah dalam topik berikut.

Daftar Isi

- Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun
- Mengaktifkan Runtime Monitoring untuk akun mandiri

Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun

Di lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan Runtime Monitoring untuk akun anggota, dan mengelola konfigurasi agen otomatis untuk jenis sumber daya milik akun anggota di organisasinya. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat Mengelola beberapa akun.

Untuk akun GuardDuty administrator yang didelegasikan

Untuk mengaktifkan Runtime Monitoring untuk akun administrator yang didelegasikan GuardDuty

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi, pilih Edit di bagian konfigurasi Runtime Monitoring.
4. Menggunakan Aktifkan untuk semua akun

   Jika Anda ingin mengaktifkan Runtime Monitoring untuk semua akun milik organisasi, termasuk akun GuardDuty administrator yang didelegasikan, pilih Aktifkan untuk semua akun.

5. Menggunakan Konfigurasi akun secara manual

   Jika Anda ingin mengaktifkan Runtime Monitoring untuk setiap akun anggota satu per satu, lalu pilih Konfigurasi akun secara manual.

   - Pilih Aktifkan di bawah bagian Administrator Delegasi (akun ini).

6. Kelola agen keamanan untuk jenis sumber daya Anda. Untuk informasi selengkapnya, lihat Mengelola agen GuardDuty keamanan.

Untuk semua akun anggota

Untuk mengaktifkan Runtime Monitoring untuk semua akun anggota di organisasi

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Masuk menggunakan akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Runtime Monitoring.
3. Pada halaman Runtime Monitoring, di bawah tab Configuration, pilih Edit di bagian konfigurasi Runtime Monitoring.
4. Pilih Aktifkan untuk semua akun.
5. Kelola agen keamanan untuk jenis sumber daya Anda. Untuk informasi selengkapnya, lihat Mengelola agen GuardDuty keamanan.

Untuk semua akun anggota aktif yang ada

Untuk mengaktifkan Runtime Monitoring untuk akun anggota yang ada di organisasi

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Masuk menggunakan akun GuardDuty administrator yang didelegasikan untuk organisasi.

2. Di panel navigasi, pilih Runtime Monitoring.
3. Pada halaman Runtime Monitoring, di bawah tab Configuration, Anda dapat melihat status konfigurasi Runtime Monitoring saat ini.
4. Dalam panel Runtime Monitoring, di bawah bagian Account anggota aktif, pilih Tindakan.
5. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.

6. Pilih Konfirmasi.
7. Kelola agen keamanan untuk jenis sumber daya Anda. Untuk informasi selengkapnya, lihat Mengelola agen GuardDuty keamanan.

> **Note**
>
> Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Auto-enable Runtime Monitoring hanya untuk akun anggota baru

Untuk mengaktifkan Runtime Monitoring untuk akun anggota baru di organisasi Anda

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Masuk menggunakan akun GuardDuty administrator organisasi yang didelegasikan yang ditunjuk.
2. Di panel navigasi, pilih Runtime Monitoring
3. Di bawah tab Konfigurasi, pilih Edit di bagian konfigurasi Runtime Monitoring.
4. Pilih Konfigurasikan akun secara manual.
5. Pilih Aktifkan secara otomatis untuk akun anggota baru.
6. Kelola agen keamanan untuk jenis sumber daya Anda. Untuk informasi selengkapnya, lihat Mengelola agen GuardDuty keamanan.

Hanya untuk akun anggota aktif selektif

Untuk mengaktifkan Runtime Monitoring untuk akun anggota aktif individu

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.
2. Di panel navigasi, pilih Akun.
3. Pada halaman Akun, tinjau nilai di kolom Runtime Monitoring dan Manage agent secara otomatis. Nilai-nilai ini menunjukkan apakah Runtime Monitoring dan manajemen GuardDuty agen Diaktifkan atau Tidak diaktifkan untuk akun terkait.

4. Dari tabel Akun, pilih akun yang ingin Anda aktifkan Runtime Monitoring. Anda dapat memilih beberapa akun sekaligus.
5. Pilih Konfirmasi.
6. Pilih Edit paket perlindungan. Pilih tindakan yang sesuai.
7. Pilih Konfirmasi.
8. Kelola agen keamanan untuk jenis sumber daya Anda. Untuk informasi selengkapnya, lihat Mengelola agen GuardDuty keamanan.

Mengaktifkan Runtime Monitoring untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun.

Setelah Anda mengaktifkan Runtime Monitoring, pastikan untuk menginstal agen GuardDuty keamanan melalui konfigurasi otomatis atau penerapan manual. Sebagai bagian dari menyelesaikan semua langkah yang tercantum dalam prosedur berikut, pastikan untuk menginstal agen keamanan.

Untuk mengaktifkan Runtime Monitoring di akun mandiri

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi, pilih Aktifkan untuk mengaktifkan Runtime Monitoring untuk akun Anda.
4. Kelola agen keamanan untuk jenis sumber daya Anda. Untuk informasi selengkapnya, lihat Mengelola agen GuardDuty keamanan.

Mengelola agen GuardDuty keamanan

Anda dapat mengelola agen GuardDuty keamanan untuk sumber daya yang ingin Anda pantau. Jika Anda ingin memantau lebih dari satu jenis sumber daya, pastikan untuk mengelola GuardDuty agen untuk sumber daya tersebut.

Topik berikut akan membantu Anda dengan langkah selanjutnya untuk mengelola agen keamanan.

Daftar Isi

- Mengaktifkan agen keamanan otomatis untuk instans Amazon EC2
- Mengelola agen keamanan secara manual untuk sumber daya Amazon EC2
- Mengelola agen GuardDuty keamanan di Bottlerocket (Amazon ECS di Amazon EC2)
- Mengelola agen keamanan otomatis untuk Fargate (hanya Amazon ECS)
- Mengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS
- Mengelola agen keamanan secara manual untuk klaster Amazon EKS
- Konfigurasikan parameter agen GuardDuty keamanan (add-on) untuk Amazon EKS
- Memvalidasi konfigurasi titik akhir VPC

Mengaktifkan agen keamanan otomatis untuk instans Amazon EC2

Bagian ini mencakup langkah-langkah untuk mengaktifkan agen GuardDuty otomatis untuk sumber daya Amazon EC2 Anda di akun mandiri Anda atau lingkungan beberapa akun.

Sebelum Anda melanjutkan, pastikan untuk mengikuti semuaPrasyarat untuk dukungan instans Amazon EC2.

Topik

- Mengaktifkan GuardDuty agen untuk sumber daya Amazon EC2 di lingkungan multi-akun
- Mengaktifkan agen GuardDuty otomatis untuk sumber daya Amazon EC2 di akun mandiri
- Migrasi dari agen manual Amazon EC2 ke agen otomatis

Jika Anda bermigrasi dari mengelola GuardDuty agen secara manual ke mengaktifkan agen GuardDuty otomatis, maka sebelum mengikuti langkah-langkah untuk mengaktifkan agen GuardDuty otomatis, lihat. Migrasi dari agen manual Amazon EC2 ke agen otomatis

Mengaktifkan GuardDuty agen untuk sumber daya Amazon EC2 di lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan konfigurasi agen otomatis untuk jenis sumber daya milik akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi

ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat Mengelola beberapa akun.

Untuk akun GuardDuty administrator yang didelegasikan

Configure for all instances

Jika Anda memilih Aktifkan untuk semua akun untuk Runtime Monitoring, pilih salah satu opsi berikut untuk akun GuardDuty administrator yang didelegasikan:

- Opsi 1

  Di bawah Konfigurasi agen otomatis, di bagian EC2, pilih Aktifkan untuk semua akun.
- Opsi 2
  - Di bawah Konfigurasi agen otomatis, di bagian EC2, pilih Konfigurasi akun secara manual.
  - Di bawah Administrator Delegasi (akun ini), pilih Aktifkan.
- Pilih Simpan.

Jika Anda memilih Konfigurasi akun secara manual untuk Runtime Monitoring, lakukan langkah-langkah berikut:

- Di bawah Konfigurasi agen otomatis, di bagian EC2, pilih Konfigurasi akun secara manual.
- Di bawah Administrator Delegasi (akun ini), pilih Aktifkan.
- Pilih Simpan.

Terlepas dari opsi mana yang Anda pilih untuk mengaktifkan konfigurasi agen otomatis untuk akun GuardDuty administrator yang didelegasikan, Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan pada semua sumber daya EC2 milik akun ini.

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Buka tab Target untuk asosiasi SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

Using inclusion tag in selected instances

Untuk mengonfigurasi GuardDuty agen untuk instans Amazon EC2 yang dipilih

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Tambahkan `true` tag`GuardDutyManaged`: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat Untuk menambahkan tag ke sumber daya individual.

   Menambahkan tag ini akan memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk instans EC2 yang dipilih ini. Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.
3. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan hanya pada sumber daya EC2 yang ditandai dengan tag inklusi.

   Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.

   - Buka tab Target untuk asosiasi SSM yang akan dibuat (`GuardDutyRuntimeMonitoring-do-not-delete`). Tombol Tag muncul sebagai tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Pastikan Anda menambahkan tag pengecualian ke instans Amazon EC2 sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2, instans EC2 apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen otomatis. GuardDuty

Untuk mengonfigurasi GuardDuty agen untuk instans Amazon EC2 yang dipilih

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

2. Tambahkan `false` tag`GuardDutyManaged`: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat Untuk menambahkan tag ke sumber daya individual.
3. Untuk tag pengecualian akan tersedia dalam metadata contoh, lakukan langkah-langkah berikut:

    a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.

    Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.

    b. Di bawah menu Tindakan, pilih Pengaturan instans.

    c. Pilih Izinkan tag dalam metadata contoh.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilai runtimeCakupan runtime dan pemecahan masalah untuk instans Amazon EC2.

Auto-enable untuk semua akun anggota

> **Note**
>
> Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Configure for all instances

Langkah-langkah berikut mengasumsikan bahwa Anda memilih Aktifkan untuk semua akun di bagian Runtime Monitoring:

1. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis untuk Amazon EC2.
2. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat (`GuardDutyRuntimeMonitoring-do-not-delete`) akan menginstal dan mengelola agen keamanan pada semua sumber daya EC2 milik akun ini.

    a. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.

b. Buka tab Target untuk asosiasi SSM. Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

Using inclusion tag in selected instances

Untuk mengonfigurasi GuardDuty agen untuk instans Amazon EC2 yang dipilih

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Tambahkan `true` tag`GuardDutyManaged`: ke instans EC2 yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat Untuk menambahkan tag ke sumber daya individual.

   Menambahkan tag ini akan memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk instans EC2 yang dipilih ini. Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.
3. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan pada semua sumber daya EC2 milik akun Anda.

   a. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.

   b. Buka tab Target untuk asosiasi SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

Using exclusion tag in selected instances

> **Note**
>
> Pastikan Anda menambahkan tag pengecualian ke instans Amazon EC2 sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2, instans EC2 apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen otomatis. GuardDuty

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans Amazon EC2 yang dipilih

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Tambahkan `false` tag`GuardDutyManaged`: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat Untuk menambahkan tag ke sumber daya individual.
3. Untuk tag pengecualian akan tersedia dalam metadata contoh, lakukan langkah-langkah berikut:

   a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.

      Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.

   b. Di bawah menu Tindakan, pilih Pengaturan instans.

   c. Pilih Izinkan tag dalam metadata contoh.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilai runtimeCakupan runtime dan pemecahan masalah untuk instans Amazon EC2.

Auto-enable hanya untuk akun anggota baru

Akun GuardDuty administrator yang didelegasikan dapat mengatur konfigurasi agen otomatis untuk sumber daya Amazon EC2 agar secara otomatis mengaktifkan akun anggota baru saat mereka bergabung dengan organisasi.

Configure for all instances

Langkah-langkah berikut mengasumsikan bahwa Anda memilih Aktifkan secara otomatis untuk akun anggota baru di bawah bagian Runtime Monitoring:

1. Di panel navigasi, pilih Runtime Monitoring.
2. Pada halaman Runtime Monitoring, pilih Edit.
3. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, konfigurasi agen otomatis untuk

Amazon EC2 akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator organisasi yang didelegasikan yang dapat mengubah pilihan ini.

4. Pilih Simpan.

Ketika akun anggota baru bergabung dengan organisasi, konfigurasi ini akan diaktifkan untuk mereka secara otomatis. GuardDuty Untuk mengelola agen keamanan untuk instans Amazon EC2 milik akun anggota baru ini, pastikan semua prasyarat Untuk contoh EC2 terpenuhi.

Ketika asosiasi SSM dibuat (`GuardDutyRuntimeMonitoring-do-not-delete`), Anda dapat memverifikasi bahwa asosiasi SSM akan menginstal dan mengelola agen keamanan pada semua instans EC2 milik akun anggota baru.

- Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
- Buka tab Target untuk asosiasi SSM. Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

Using inclusion tag in selected instances

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans yang dipilih di akun Anda

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Tambahkan `true` tag`GuardDutyManaged`: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat Untuk menambahkan tag ke sumber daya individual.

   Menambahkan tag ini akan memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk instance yang dipilih ini. Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.
3. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan hanya pada sumber daya EC2 yang ditandai dengan tag inklusi.

   a. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.

   b. Buka tab Target untuk asosiasi SSM yang akan dibuat. Tombol Tag muncul sebagai tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Pastikan Anda menambahkan tag pengecualian ke instans Amazon EC2 sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2, instans EC2 apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen otomatis. GuardDuty

Untuk mengonfigurasi agen GuardDuty keamanan untuk instance tertentu di akun mandiri Anda

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Tambahkan `false` tag`GuardDutyManaged`: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat Untuk menambahkan tag ke sumber daya individual.
3. Untuk tag pengecualian akan tersedia dalam metadata contoh, lakukan langkah-langkah berikut:

   a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.

      Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.

   b. Di bawah menu Tindakan, pilih Pengaturan instans.

   c. Pilih Izinkan tag dalam metadata contoh.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilai runtimeCakupan runtime dan pemecahan masalah untuk instans Amazon EC2.

Hanya akun anggota selektif

Configure for all instances

1. Pada halaman Akun, pilih satu atau beberapa akun yang ingin Anda aktifkan konfigurasi Monitoring-Automated agen Runtime (Amazon EC2). Pastikan akun yang Anda pilih pada langkah ini sudah mengaktifkan Runtime Monitoring.
2. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi Monitoring-Automated agen Runtime (Amazon EC2).
3. Pilih Konfirmasi.

Using inclusion tag in selected instances

Untuk mengonfigurasi agen GuardDuty keamanan untuk instance yang dipilih

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Tambahkan `true` tag`GuardDutyManaged`: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat Untuk menambahkan tag ke sumber daya individual.

   Menambahkan tag ini akan memungkinkan GuardDuty untuk mengelola agen keamanan untuk instans Amazon EC2 Anda yang ditandai. Anda tidak perlu secara eksplisit mengaktifkan konfigurasi agen otomatis (Runtime Monitoring - Automated agent configuration (EC2).

Using exclusion tag in selected instances

> **Note**
>
> Pastikan Anda menambahkan tag pengecualian ke instans Amazon EC2 sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2, instans EC2 apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen otomatis. GuardDuty

Untuk mengonfigurasi agen GuardDuty keamanan untuk instance yang dipilih

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Tambahkan `false` tag`GuardDutyManaged`: ke instans EC2 yang tidak GuardDuty ingin Anda pantau atau deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat Untuk menambahkan tag ke sumber daya individual.
3. Untuk tag pengecualian akan tersedia dalam metadata contoh, lakukan langkah-langkah berikut:

   a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.

      Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.

   b. Di bawah menu Tindakan, pilih Pengaturan instans.

   c. Pilih Izinkan tag dalam metadata contoh.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilaiCakupan runtime dan pemecahan masalah untuk instans Amazon EC2.

Mengaktifkan agen GuardDuty otomatis untuk sumber daya Amazon EC2 di akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun.

Setelah Anda mengaktifkan Runtime Monitoring, pastikan untuk menginstal agen GuardDuty keamanan melalui konfigurasi otomatis atau penerapan manual. Sebagai bagian dari menyelesaikan semua langkah yang tercantum dalam prosedur berikut, pastikan untuk menginstal agen keamanan.

Berdasarkan preferensi Anda untuk memantau semua atau sumber daya Amazon EC2 selektif, pilih metode yang disukai dan ikuti langkah-langkah dalam tabel berikut.

Configure for all instances

Untuk mengonfigurasi Runtime Monitoring untuk semua instance di akun mandiri

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi, pilih Edit.
4. Di bagian EC2, pilih Aktifkan.
5. Pilih Simpan.
6. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan pada semua sumber daya EC2 milik akun Anda.

   a. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.

   b. Buka tab Target untuk asosiasi SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

Using inclusion tag in selected instances

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans Amazon EC2 yang dipilih

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Tambahkan `true` tag`GuardDutyManaged`: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat Untuk menambahkan tag ke sumber daya individual.
3. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan hanya pada sumber daya EC2 yang ditandai dengan tag inklusi.

   Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.

   - Buka tab Target untuk asosiasi SSM yang akan dibuat (`GuardDutyRuntimeMonitoring-do-not-delete`). Tombol Tag muncul sebagai tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Pastikan Anda menambahkan tag pengecualian ke instans Amazon EC2 sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2, instans EC2 apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen otomatis. GuardDuty

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans Amazon EC2 yang dipilih

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Tambahkan `false` tag`GuardDutyManaged`: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat Untuk menambahkan tag ke sumber daya individual.
3. Untuk tag pengecualian akan tersedia dalam metadata contoh, lakukan langkah-langkah berikut:

   a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.

      Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.

   b. Pilih contoh yang ingin Anda izinkan tag.

   c. Di bawah menu Tindakan, pilih Pengaturan instans.

   d. Pilih Izinkan tag dalam metadata contoh.

   e. Di bawah Akses ke tag dalam metadata instance, pilih Izinkan.

   f. Pilih Simpan.

4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan di tab Configure for all instance.

Anda sekarang dapat menilai runtimeCakupan runtime dan pemecahan masalah untuk instans Amazon EC2.

Migrasi dari agen manual Amazon EC2 ke agen otomatis

Bagian ini berlaku untuk Anda Akun AWS jika sebelumnya Anda mengelola agen keamanan secara manual dan sekarang ingin menggunakan konfigurasi agen GuardDuty otomatis. Jika ini tidak berlaku untuk Anda, lanjutkan dengan mengonfigurasi agen keamanan untuk akun Anda.

Ketika Anda mengaktifkan agen GuardDuty otomatis, GuardDuty mengelola agen keamanan atas nama Anda. Untuk informasi tentang langkah-langkah apa yang GuardDuty diambil, lihatKonfigurasi agen otomatis (disarankan).

Pembersihan sumber daya

Hapus asosiasi SSM

- Hapus asosiasi SSM apa pun yang mungkin telah Anda buat saat mengelola agen keamanan untuk Amazon EC2 secara manual. Untuk informasi selengkapnya, lihat Menghapus asosiasi.
- Hal ini dilakukan agar GuardDuty dapat mengambil alih pengelolaan tindakan SSM apakah Anda menggunakan agen otomatis di tingkat akun atau tingkat instans (dengan menggunakan tag inklusi atau pengecualian). Untuk informasi selengkapnya tentang tindakan SSM yang dapat GuardDuty dilakukan, lihatService-linked izin peran untuk GuardDuty.
- Ketika Anda menghapus asosiasi SSM yang sebelumnya dibuat untuk mengelola agen keamanan secara manual, mungkin ada periode singkat tumpang tindih ketika GuardDuty membuat asosiasi SSM untuk mengelola agen keamanan secara otomatis. Selama periode ini, Anda dapat mengalami konflik berdasarkan penjadwalan SSM. Untuk informasi selengkapnya, lihat penjadwalan SSM Amazon EC2.

Mengelola tag inklusi dan pengecualian untuk instans Amazon EC2

- Tag penyertaan — Jika Anda tidak mengaktifkan konfigurasi agen GuardDuty otomatis tetapi menandai instans Amazon EC2 Anda dengan tag inklusi (`GuardDutyManaged:true`), GuardDuty buat asosiasi SSM yang akan menginstal dan mengelola agen keamanan pada instans EC2 yang dipilih. Ini adalah perilaku yang diharapkan yang membantu Anda mengelola agen keamanan pada instans EC2 tertentu saja. Untuk informasi selengkapnya, lihat Menyebarkan agen keamanan ke Amazon EC2.

  Untuk GuardDuty mencegah menginstal dan mengelola agen keamanan, hapus tag inklusi dari instans EC2 ini. Untuk informasi selengkapnya, lihat Menambahkan dan menghapus tag di Panduan Pengguna Amazon EC2.

- Tag pengecualian — Saat Anda ingin mengaktifkan konfigurasi agen GuardDuty otomatis untuk semua instans EC2 di akun Anda, pastikan tidak ada instans EC2 yang ditandai dengan tag pengecualian (:). `GuardDutyManaged false`

Mengelola agen keamanan secara manual untuk sumber daya Amazon EC2

Bagian ini menyediakan langkah-langkah untuk menginstal dan memperbarui agen keamanan secara manual untuk sumber daya Amazon EC2 Anda.

Setelah Anda mengaktifkan Runtime Monitoring, Anda harus menginstal agen GuardDuty keamanan secara manual. Untuk mengelola agen GuardDuty keamanan secara manual, Anda harus terlebih dahulu membuat endpoint Amazon VPC secara manual. Setelah ini, Anda dapat menginstal agen keamanan sehingga GuardDuty akan mulai menerima peristiwa runtime dari instans Amazon EC2. Saat GuardDuty merilis versi agen baru untuk sumber daya ini, Anda dapat memperbarui versi agen di akun Anda.

Topik berikut mencakup langkah-langkah untuk terus mengelola agen keamanan untuk sumber daya Amazon EC2 Anda.

Topik

- Prasyarat - Membuat titik akhir Amazon VPC secara manual
- Memasang agen keamanan secara manual
- Memperbarui agen GuardDuty keamanan untuk instans Amazon EC2 secara manual

Prasyarat - Membuat titik akhir Amazon VPC secara manual

Sebelum Anda dapat menginstal agen GuardDuty keamanan, Anda harus membuat titik akhir Amazon Virtual Private Cloud (Amazon VPC). Ini akan membantu GuardDuty menerima peristiwa runtime instans Amazon EC2 Anda.

> **Note**
>
> Tidak ada biaya tambahan untuk penggunaan titik akhir VPC.

Untuk membuat titik akhir VPC Amazon

1. Masuk ke Konsol Manajemen AWS dan buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, di bawah VPC private cloud, pilih Endpoints.
3. Pilih Buat Titik Akhir.
4. Pada halaman Buat titik akhir, untuk kategori Layanan, pilih Layanan titik akhir lainnya.
5. Untuk nama Layanan, masukkan**com.amazonaws.*us-east-1*.guardduty-data**.

   Pastikan untuk mengganti *us-east-1* dengan Anda Wilayah AWS. Ini harus Wilayah yang sama dengan instans Amazon EC2 yang termasuk dalam ID AWS akun Anda.
6. Pilih Verifikasi layanan.
7. Setelah nama layanan berhasil diverifikasi, pilih VPC tempat instans Anda berada. Tambahkan kebijakan berikut untuk membatasi penggunaan titik akhir VPC Amazon hanya ke akun yang ditentukan. Dengan organisasi yang `Condition` disediakan di bawah kebijakan ini, Anda dapat memperbarui kebijakan berikut untuk membatasi akses ke titik akhir Anda. Untuk memberikan dukungan endpoint Amazon VPC ke ID akun tertentu di organisasi Anda, lihat. Organization condition to restrict access to your endpoint

   JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
```

```
    "Principal": "*"
   }
  ]
}
```

ID `aws:PrincipalAccount` akun harus cocok dengan akun yang berisi titik akhir VPC dan VPC. Daftar berikut menunjukkan cara berbagi titik akhir VPC dengan ID akun lain AWS :

- Untuk menentukan beberapa akun untuk mengakses titik akhir VPC, ganti `"aws:PrincipalAccount: "111122223333"` dengan blok berikut:

  ```
  "aws:PrincipalAccount": [
            "666666666666",
            "555555555555"
       ]
  ```

  Pastikan untuk mengganti ID AWS akun dengan ID akun dari akun yang perlu mengakses titik akhir VPC.

- Untuk mengizinkan semua anggota dari organisasi mengakses titik akhir VPC, ganti `"aws:PrincipalAccount: "111122223333"` dengan baris berikut:

  ```
  "aws:PrincipalOrgID": "o-abcdef0123"
  ```

  Pastikan untuk mengganti organisasi *o-abcdef0123* dengan ID organisasi Anda.

- Untuk membatasi akses sumber daya dengan ID organisasi, tambahkan `ResourceOrgID` ke kebijakan. Untuk informasi lebih lanjut, lihat `aws:ResourceOrgID` dalam Panduan Pengguna IAM.

  ```
  "aws:ResourceOrgID": "o-abcdef0123"
  ```

8. Di bawah Pengaturan tambahan, pilih Aktifkan nama DNS.
9. Di bawah Subnet, pilih subnet tempat instans Anda berada.
10. Di bawah Grup keamanan, pilih grup keamanan yang mengaktifkan port 443 dalam terikat dari VPC Anda (atau instans Amazon EC2 Anda). Jika Anda belum memiliki grup keamanan yang mengaktifkan port 443 dalam ikatan, lihat Membuat grup keamanan untuk VPC Anda di Panduan Pengguna Amazon VPC.

Jika ada masalah saat membatasi izin masuk ke VPC (atau instance), Anda dapat menggunakan port 443 yang di-bound dari alamat IP apa pun. `(0.0.0.0/0)` Namun, GuardDuty rekomendasikan untuk menggunakan alamat IP yang cocok dengan blok CIDR untuk VPC Anda. Untuk informasi selengkapnya, lihat blok CIDR VPC di Panduan Pengguna Amazon VPC.

Setelah Anda mengikuti langkah-langkahnya, lihat Memvalidasi konfigurasi titik akhir VPC untuk memastikan bahwa titik akhir VPC telah diatur dengan benar.

Memasang agen keamanan secara manual

GuardDuty menyediakan dua metode berikut untuk menginstal agen GuardDuty keamanan di instans Amazon EC2 Anda. Sebelum melanjutkan, pastikan untuk mengikuti langkah-langkah di bawah Prasyarat - Membuat titik akhir Amazon VPC secara manual ini.

Pilih metode akses yang disukai untuk menginstal agen keamanan di sumber daya Amazon EC2 Anda.

- Metode 1 - Menggunakan AWS Systems Manager— Metode ini mengharuskan instans Amazon EC2 Anda dikelola. AWS Systems Manager
- Metode 2 - Menggunakan Linux Package Manager— Anda dapat menggunakan metode ini apakah instans Amazon EC2 Anda dikelola atau tidak. AWS Systems Manager Berdasarkan distribusi OS Anda, Anda dapat memilih metode yang sesuai untuk menginstal skrip RPM atau skrip Debian. Jika Anda menggunakan platform Fedora, maka Anda harus menggunakan metode ini untuk menginstal agen.

Metode 1 - Menggunakan AWS Systems Manager

Untuk menggunakan metode ini, pastikan instans Amazon EC2 Anda AWS Systems Manager dikelola dan kemudian instal agen.

AWS Systems Manager instans Amazon EC2 yang dikelola

Gunakan langkah-langkah berikut untuk membuat instans AWS Systems Manager Amazon EC2 Anda dikelola.

- AWS Systems Managermembantu Anda mengelola AWS aplikasi dan sumber daya secara end-to-end dan mengaktifkan operasi yang aman dalam skala besar.

Untuk mengelola instans Amazon EC2 Anda AWS Systems Manager, lihat Menyiapkan Systems Manager untuk instans Amazon EC2 di Panduan Pengguna.AWS Systems Manager

- Tabel berikut menunjukkan AWS Systems Manager dokumen GuardDuty terkelola baru:

Nama dokumen	Jenis dokumen	Tujuan
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	Distributor	Untuk mengemas agen GuardDuty keamanan.
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Perintah	Untuk menjalankan skrip installation/un -installation untuk menginstal agen GuardDuty keamanan.

Untuk informasi selengkapnya AWS Systems Manager, lihat Dokumen Amazon EC2 Systems Manager di AWS Systems Manager Panduan Pengguna.

> **Untuk Server Debian**
>
> Amazon Machine Images (AMI) untuk Debian Server yang disediakan oleh AWS mengharuskan Anda untuk menginstal AWS Systems Manager agen (agen SSM). Anda perlu melakukan langkah tambahan untuk menginstal agen SSM untuk membuat instans Amazon EC2 Debian Server SSM dikelola. Untuk informasi tentang langkah-langkah yang perlu Anda ambil, lihat Menginstal agen SSM secara manual pada instance Server Debian di Panduan Pengguna.AWS Systems Manager

Untuk menginstal GuardDuty agen untuk instans Amazon EC2 dengan menggunakan AWS Systems Manager

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, pilih Dokumen
3. Di Dimiliki oleh Amazon, pilih`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.

4. Pilih Run Command.
5. Masukkan parameter Run Command berikut

   - Tindakan: Pilih Instal.
   - Jenis Instalasi: Pilih Install atau Uninstall.
   - Nama: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
   - Versi: Jika ini tetap kosong, Anda akan mendapatkan versi terbaru dari agen GuardDuty keamanan. Untuk informasi lebih lanjut tentang versi rilis,GuardDuty versi agen keamanan untuk instans Amazon EC2.
6. Pilih instans Amazon EC2 yang ditargetkan. Anda dapat memilih satu atau beberapa instans Amazon EC2. Untuk informasi selengkapnya, lihat AWS Systems Manager Menjalankan perintah dari konsol di Panduan AWS Systems Manager Pengguna
7. Validasi jika instalasi GuardDuty agen sehat. Untuk informasi selengkapnya, lihat Memvalidasi status instalasi agen GuardDuty keamanan.

Metode 2 - Menggunakan Linux Package Manager

Dengan metode ini, Anda dapat menginstal agen GuardDuty keamanan dengan menjalankan skrip RPM atau skrip Debian. Berdasarkan sistem operasi, Anda dapat memilih metode yang disukai:

- Gunakan skrip RPM untuk menginstal agen keamanan pada distribusi OS AL2, AL2023,, CentOS, atau Fedora. RedHat
- Gunakan skrip Debian untuk menginstal agen keamanan pada distribusi OS Ubuntu atau Debian. Untuk informasi tentang distribusi Ubuntu dan Debian OS yang didukung, lihat. Validasi persyaratan arsitektur

RPM installation

> **Important**
>
> Sebaiknya verifikasi tanda tangan RPM agen GuardDuty keamanan sebelum menginstalnya di mesin Anda.

1. Verifikasi tanda tangan RPM agen GuardDuty keamanan

a. Siapkan template

Siapkan perintah dengan kunci publik yang sesuai, tanda tangan x86_64 RPM, tanda tangan arm64 RPM, dan tautan akses yang sesuai ke skrip RPM yang dihosting di bucket Amazon S3. Ganti nilai Wilayah AWS, ID AWS akun, dan versi GuardDuty agen untuk mengakses skrip RPM.

- Kunci publik:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
publickey.pem
```

- GuardDuty tanda tangan agen keamanan RPM:

  Tanda tangan dari x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
x86_64/amazon-guardduty-agent-1.17.1.x86_64.sig
```

  Tanda tangan arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/arm64/
amazon-guardduty-agent-1.17.1.arm64.sig
```

- Akses tautan ke skrip RPM di bucket Amazon S3:

  Tautan akses untuk x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
x86_64/amazon-guardduty-agent-1.17.1.x86_64.rpm
```

  Tautan akses untuk arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/arm64/
amazon-guardduty-agent-1.17.1.arm64.rpm
```

Wilayah AWS	Nama wilayah	AWS ID akun
eu-west-1	Eropa (Irlandia)	694911143906

us-east-1	AS Timur (Virginia Utara)	593207742271
us-west-2	AS Barat (Oregon)	733349766148
eu-west-3	Eropa (Paris)	665651866788
us-east-2	AS Timur (Ohio)	307168627858
eu-central-1	Eropa (Frankfurt)	323658145986
ap-northeast-2	Asia Pasifik (Seoul)	914738172881
eu-north-1	Eropa (Stockholm)	591436053604
ap-east-1	Asia Pasifik (Hong Kong)	258348409381
me-south-1	Timur Tengah (Bahrain)	536382113932
eu-west-2	Eropa (London)	892757235363
ap-northeast-1	Asia Pasifik (Tokyo)	533107202818
ap-southeast-1	Asia Pasifik (Singapura)	174946120834
ap-south-1	Asia Pasifik (Mumbai)	251508486986
ap-southeast-3	Asia Pasifik (Jakarta)	510637619217
sa-east-1	Amerika Selatan (Sao Paulo)	758426053663
ap-northeast-3	Asia Pasifik (Osaka)	273192626886
eu-south-1	Europe (Milan)	266869475730
af-south-1	Africa (Cape Town)	197869348890
ap-southeast-2	Asia Pasifik (Sydney)	005257825471
me-central-1	Timur Tengah (UAE)	000014521398

us-west-1	AS Barat (California Utara)	684579721401
ca-central-1	Kanada (Pusat)	354763396469
ca-west-1	Kanada Barat (Calgary)	339712888787
ap-south-2	Asia Pasifik (Hyderabad)	950823858135
eu-south-2	Eropa (Spanyol)	919611009337
eu-central-2	Europe (Zurich)	529164026651
ap-southeast-4	Asia Pacific (Melbourne)	251357961535
ap-southeast-7	Asia Pasifik (Thailand)	054037130133
il-central-1	Israel (Tel Aviv)	870907303882
mx-central-1	Meksiko (Tengah)	982081086614
ap-east-2	Asia Pasifik (Taipei)	259886477082

b. Unduh templatnya

Dalam perintah berikut untuk mengunduh kunci publik yang sesuai, tanda tangan x86_64 RPM, tanda tangan arm64 RPM, dan tautan akses yang sesuai ke skrip RPM yang dihosting di bucket Amazon S3, pastikan untuk mengganti ID akun dengan ID yang sesuai Akun AWS dan Wilayah dengan Wilayah Anda saat ini.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
x86_64/amazon-guardduty-agent-1.17.1.x86_64.rpm ./amazon-guardduty-
agent-1.17.1.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
x86_64/amazon-guardduty-agent-1.17.1.x86_64.sig ./amazon-guardduty-
agent-1.17.1.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
publickey.pem ./publickey.pem
```

c. Impor kunci publik

Gunakan perintah berikut untuk mengimpor kunci publik ke database:

```
gpg --import publickey.pem
```

gpg menunjukkan impor berhasil

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. Verifikasi tanda tangan

Gunakan perintah berikut untuk memverifikasi tanda tangan

```
gpg --verify amazon-guardduty-agent-1.17.1.x86_64.sig amazon-guardduty-
agent-1.17.1.x86_64.rpm
```

Jika verifikasi berlalu, Anda akan melihat pesan yang mirip dengan hasil di bawah ini. Anda sekarang dapat melanjutkan untuk menginstal agen GuardDuty keamanan menggunakan RPM.

Contoh output:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Jika verifikasi gagal, itu berarti tanda tangan pada RPM berpotensi dirusak. Anda harus menghapus kunci publik dari database dan mencoba lagi proses verifikasi.

Contoh:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Gunakan perintah berikut untuk menghapus kunci publik dari database:

```
gpg --delete-keys AwsGuardDuty
```

Sekarang, coba proses verifikasi lagi.

2. Connect dengan SSH dari Linux atau macOS.
3. Instal agen GuardDuty keamanan dengan menggunakan perintah berikut:

```
sudo rpm -ivh amazon-guardduty-agent-1.17.1.x86_64.rpm
```

4. Validasi jika instalasi GuardDuty agen sehat. Untuk informasi selengkapnya tentang langkah-langkahnya, lihatMemvalidasi status instalasi agen GuardDuty keamanan.

Debian installation

> **Important**
>
> Sebaiknya verifikasi tanda tangan agen GuardDuty keamanan Debian sebelum menginstalnya di mesin Anda.

1. Verifikasi tanda GuardDuty tangan agen keamanan Debian

   a. Siapkan template untuk kunci publik yang sesuai, tanda tangan paket Debian amd64, tanda tangan paket Debian arm64, dan tautan akses terkait ke skrip Debian yang dihosting di bucket Amazon S3

   Dalam template berikut, ganti nilai, ID AWS akun Wilayah AWS, dan versi GuardDuty agen untuk mengakses skrip paket Debian.

   - Kunci publik:

   ```
   s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/
   publickey.pem
   ```

   - GuardDuty tanda tangan agen keamanan Debian:

Tanda tangan amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/amd64/
amazon-guardduty-agent-1.17.1.amd64.sig
```

Tanda tangan arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/arm64/
amazon-guardduty-agent-1.17.1.arm64.sig
```

- Akses tautan ke skrip Debian di bucket Amazon S3:

  Tautan akses untuk amd64

  ```
  s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/amd64/
  amazon-guardduty-agent-1.17.1.amd64.deb
  ```

  Tautan akses untuk arm64

  ```
  s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/arm64/
  amazon-guardduty-agent-1.17.1.arm64.deb
  ```

Wilayah AWS	Nama wilayah	AWS ID akun
eu-west-1	Eropa (Irlandia)	694911143906
us-east-1	AS Timur (Virginia Utara)	593207742271
us-west-2	AS Barat (Oregon)	733349766148
eu-west-3	Eropa (Paris)	665651866788
us-east-2	AS Timur (Ohio)	307168627858
eu-central-1	Eropa (Frankfurt)	323658145986
ap-northeast-2	Asia Pasifik (Seoul)	914738172881
eu-north-1	Eropa (Stockholm)	591436053604

ap-east-1	Asia Pasifik (Hong Kong)	258348409381
me-south-1	Timur Tengah (Bahrain)	536382113932
eu-west-2	Eropa (London)	892757235363
ap-northeast-1	Asia Pasifik (Tokyo)	533107202818
ap-southeast-1	Asia Pasifik (Singapura)	174946120834
ap-south-1	Asia Pasifik (Mumbai)	251508486986
ap-southeast-3	Asia Pasifik (Jakarta)	510637619217
sa-east-1	Amerika Selatan (Sao Paulo)	758426053663
ap-northeast-3	Asia Pasifik (Osaka)	273192626886
eu-south-1	Europe (Milan)	266869475730
af-south-1	Africa (Cape Town)	197869348890
ap-southeast-2	Asia Pasifik (Sydney)	005257825471
me-central-1	Timur Tengah (UAE)	000014521398
us-west-1	AS Barat (California Utara)	684579721401
ca-central-1	Kanada (Pusat)	354763396469
ca-west-1	Kanada Barat (Calgary)	339712888787
ap-south-2	Asia Pasifik (Hyderabad)	950823858135
eu-south-2	Eropa (Spanyol)	919611009337
eu-central-2	Europe (Zurich)	529164026651
ap-southeast-4	Asia Pacific (Melbourne)	251357961535

il-central-1	Israel (Tel Aviv)	870907303882
mx-central-1	Meksiko (Tengah)	982081086614
ap-east-2	Asia Pasifik (Taipei)	259886477082

b. Unduh kunci publik yang sesuai, tanda tangan amd64, tanda tangan arm64, dan tautan akses yang sesuai ke skrip Debian yang dihosting di bucket Amazon S3

Dalam perintah berikut, ganti ID akun dengan ID yang sesuai Akun AWS , dan Wilayah dengan Wilayah Anda saat ini.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/
amd64/amazon-guardduty-agent-1.17.1.amd64.deb ./amazon-guardduty-
agent-1.17.1.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/
amd64/amazon-guardduty-agent-1.17.1.amd64.sig ./amazon-guardduty-
agent-1.17.1.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/
publickey.pem ./publickey.pem
```

c. Impor kunci publik ke database

```
gpg --import publickey.pem
```

gpg menunjukkan impor berhasil

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. Verifikasi tanda tangan

```
gpg --verify amazon-guardduty-agent-1.17.1.amd64.sig amazon-guardduty-
agent-1.17.1.amd64.deb
```

Setelah verifikasi berhasil, Anda akan melihat pesan yang mirip dengan hasil berikut:

Contoh output:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
```

```
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Anda sekarang dapat melanjutkan untuk menginstal agen GuardDuty keamanan menggunakan Debian.

Namun, jika verifikasi gagal, itu berarti tanda tangan dalam paket Debian berpotensi dirusak.

Contoh:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Gunakan perintah berikut untuk menghapus kunci publik dari database:

```
gpg --delete-keys AwsGuardDuty
```

Sekarang, coba lagi proses verifikasi.

2. Connect dengan SSH dari Linux atau macOS.
3. Instal agen GuardDuty keamanan dengan menggunakan perintah berikut:

```
sudo dpkg -i amazon-guardduty-agent-1.17.1.amd64.deb
```

4. Validasi jika instalasi GuardDuty agen sehat. Untuk informasi selengkapnya tentang langkah-langkahnya, lihatMemvalidasi status instalasi agen GuardDuty keamanan.

Kesalahan kehabisan memori

Jika Anda mengalami `out-of-memory` kesalahan saat menginstal atau memperbarui agen GuardDuty keamanan untuk Amazon EC2 secara manual, lihat. Memecahkan masalah kesalahan memori

Memvalidasi status instalasi agen GuardDuty keamanan

Setelah Anda melakukan langkah-langkah untuk menginstal agen GuardDuty keamanan, gunakan langkah-langkah berikut untuk memvalidasi status agen:

Untuk memvalidasi jika agen GuardDuty keamanan sehat

1. Connect dengan SSH dari Linux atau macOS.
2. Jalankan perintah berikut untuk memeriksa status agen GuardDuty keamanan:

```
sudo systemctl status amazon-guardduty-agent
```

Jika Anda ingin melihat log instalasi agen keamanan, mereka tersedia di bawah`/var/log/amzn-guardduty-agent/`.

Untuk melihat log, lakukan`sudo journalctl -u amazon-guardduty-agent`.

Memperbarui agen GuardDuty keamanan untuk instans Amazon EC2 secara manual

GuardDuty merilis pembaruan ke versi agen keamanan. Saat mengelola agen keamanan secara manual, Anda bertanggung jawab untuk memperbarui agen untuk instans Amazon EC2 Anda. Untuk informasi tentang versi agen baru, lihat GuardDuty versi rilis agen keamanan instans Amazon EC2. Untuk menerima pemberitahuan tentang rilis versi agen baru, lihatBerlangganan pengumuman Amazon GuardDuty SNS.

Untuk memperbarui agen keamanan untuk instans Amazon EC2 secara manual

Proses untuk memperbarui agen keamanan sama dengan menginstal agen keamanan. Bergantung pada metode yang Anda gunakan untuk menginstal agen, Anda dapat melakukan langkah-langkah Memasang agen keamanan secara manual untuk instans Amazon EC2.

Jika Anda menggunakan Metode 1 - Dengan menggunakan AWS Systems Manager, maka Anda dapat memperbarui agen keamanan dengan menggunakan perintah Run. Gunakan versi agen yang ingin Anda perbarui.

Jika Anda menggunakan Metode 2 - Dengan menggunakan Linux Package Managers, Anda dapat menggunakan skrip seperti yang ditentukan di Memasang agen keamanan secara manual bagian. Skrip sudah menyertakan versi rilis agen terbaru. Untuk informasi tentang versi agen yang baru dirilis, lihatGuardDuty versi agen keamanan untuk instans Amazon EC2.

Setelah Anda memperbarui agen keamanan, Anda dapat memeriksa status instalasi dengan melihat log. Untuk informasi selengkapnya, lihat Memvalidasi status instalasi agen GuardDuty keamanan.

Mengelola agen GuardDuty keamanan di Bottlerocket (Amazon ECS di Amazon EC2)

Important

Halaman ini hanya berlaku untuk versi ECS-optimized AMI Bottlerocket `v1.62.1` dan yang lebih baru, termasuk varian berikut:

- `bottlerocket-aws-ecs-2-x86_64` / `bottlerocket-aws-ecs-2-aarch64`
- `bottlerocket-aws-ecs-3-x86_64` / `bottlerocket-aws-ecs-3-aarch64`
- `bottlerocket-aws-ecs-2-nvidia` / `bottlerocket-aws-ecs-2-nvidia-fips`
- `bottlerocket-aws-ecs-3-nvidia` / `bottlerocket-aws-ecs-3-nvidia-fips`

Untuk instans Bottlerocket di kluster Amazon EKS, Runtime Monitoring menggunakan penyiapan yang berbeda. Lihat Prasyarat untuk dukungan klaster Amazon EKS.

Halaman ini menjelaskan bagaimana agen GuardDuty keamanan berjalan di ECS-optimized AMI Bottlerocket dan bagaimana menyebarkannya. GuardDuty Pada Bottlerocket, agen berjalan sebagai wadah host daripada sebagai paket RPM atau Debian yang diinstal. Bottlerocket adalah OS Linux yang dioptimalkan kontainer dengan sistem file root yang tidak dapat diubah, sehingga tidak menggunakan manajer paket tradisional. GuardDuty meng-host image container agen dalam repositori Amazon Elastic Container Registry (Amazon ECR) yang dikelola, dan saat Anda mengaktifkan Runtime Monitoring dengan konfigurasi agen otomatis GuardDuty , AWS Systems Manager gunakan Distributor untuk menyebarkan container host agen untuk Anda.

Prasyarat

Sebelum Anda melanjutkan, pastikan untuk mengikuti semuaPrasyarat untuk dukungan Bottlerocket ECS-EC2.

Mengaktifkan konfigurasi agen otomatis

ECS-EC2 Instans Bottlerocket menggunakan dokumen SSM dan konfigurasi agen otomatis yang sama dengan instans Amazon EC2 standar. Untuk mengaktifkan agen GuardDuty otomatis untuk

instans Bottlerocket Anda, ikuti langkah-langkahnya. Agen otomatis pada sumber daya Amazon EC2 Hal ini mencakup:

- Mengaktifkan GuardDuty agen di lingkungan multi-akun.
- Mengaktifkan agen GuardDuty otomatis di akun mandiri.

Untuk prasyarat tambahan saat menggunakan tag inklusi atau pengecualian, lihat. Saat menggunakan konfigurasi agen otomatis

Memverifikasi agen

Setelah mengaktifkan konfigurasi agen otomatis, verifikasi agen berjalan pada instance Bottlerocket Anda:

1. Connect ke instans Anda menggunakan SSM Session Manager.
2. Masukkan wadah admin:`enter-admin-container`.
3. Periksa log agen menggunakan salah satu dari berikut ini:
   - `sheltie journalctl -u host-containers@amazon-guardduty-agent`
   - Dari sesi sheltie (`sudo sheltie`):`ls /var/log/amzn-guardduty-agent/`.

Untuk informasi tentang meninjau statistik cakupan untuk instans Amazon EC2 Anda, lihat. Meninjau statistik cakupan

Jika status pertanggungan muncul sebagai Tidak Sehat, lihatMemecahkan masalah cakupan runtime Bottlerocket ECS-EC2.

Mengelola agen keamanan otomatis untuk Fargate (hanya Amazon ECS)

Runtime Monitoring mendukung pengelolaan agen keamanan untuk cluster Amazon ECS (AWS Fargate) Anda hanya melalui. GuardDuty Tidak ada dukungan untuk mengelola agen keamanan secara manual di cluster Amazon ECS.

Sebelum melanjutkan dengan langkah-langkah di bagian ini, pastikan untuk mengikutiPrasyarat untuk AWS Fargate (Hanya Amazon ECS) dukungan.

Berdasarkan pendekatan diMenyebarkan agen keamanan ke Amazon ECS di Fargate, pilih metode yang disukai untuk mengaktifkan agen GuardDuty otomatis untuk sumber daya Anda.

Mengkonfigurasi GuardDuty agen untuk lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan konfigurasi agen otomatis untuk akun anggota, dan mengelola konfigurasi agen otomatis untuk klaster Amazon ECS milik akun anggota di organisasinya. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat Mengelola beberapa akun di GuardDuty.

Mengaktifkan konfigurasi agen otomatis untuk akun administrator yang didelegasikan GuardDuty

Manage for all Amazon ECS clusters (account level)

Jika Anda memilih Aktifkan untuk semua akun untuk Runtime Monitoring, maka Anda memiliki opsi berikut:

- Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua tugas Amazon ECS yang diluncurkan.
- Pilih Konfigurasikan akun secara manual.

Jika Anda memilih Konfigurasi akun secara manual di bagian Runtime Monitoring, lakukan hal berikut:

1. Pilih Konfigurasi akun secara manual di bagian Konfigurasi agen otomatis.
2. Pilih Aktifkan di bagian akun GuardDuty administrator yang didelegasikan (akun ini).

Pilih Simpan.

Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.

- UpdateServicedi Referensi API Layanan Amazon Elastic Container.
- update-service di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS ini dengan pasangan nilai kunci sebagai -. `GuardDutyManaged` `false`
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
```

```
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
```

```
}
```

3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
4. Di panel navigasi, pilih Runtime Monitoring.
5.

> **Note**
>
> Selalu tambahkan tag pengecualian ke kluster Amazon ECS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

   Di bawah tab Konfigurasi, pilih Aktifkan dalam konfigurasi agen otomatis.

   Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.
6. Pilih Simpan.
7. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus `GuardDutyManaged` -. `true`
2. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Saat menggunakan tag inklusi untuk kluster Amazon ECS, Anda tidak perlu mengaktifkan GuardDuty agen melalui kongifurasi agen otomatis secara eksplisit.

3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan

Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
- UpdateServicedi Referensi API Layanan Amazon Elastic Container.
- update-service di Command Reference.AWS CLI

Auto-enable untuk semua akun anggota

Manage for all Amazon ECS clusters (account level)

Langkah-langkah berikut mengasumsikan bahwa Anda memilih Aktifkan untuk semua akun di bagian Runtime Monitoring.

1. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua tugas Amazon ECS yang diluncurkan.
2. Pilih Simpan.
3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS ini dengan pasangan nilai kunci sebagai -. `GuardDutyManaged` `false`
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
4. Di panel navigasi, pilih Runtime Monitoring.

5.
> **Note**
>
> Selalu tambahkan tag pengecualian ke kluster Amazon ECS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

   Di bawah tab Konfigurasi, pilih Edit.

6. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis

   Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

7. Pilih Simpan.

8. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Terlepas dari cara Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau tugas Amazon ECS Fargate selektif untuk semua akun anggota di organisasi Anda.

1. Jangan aktifkan konfigurasi apa pun di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang Anda pilih pada langkah sebelumnya.
2. Pilih Simpan.

3. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
```

```
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Saat menggunakan tag inklusi untuk kluster Amazon ECS, Anda tidak perlu mengaktifkan manajemen otomatis GuardDuty agen secara eksplisit.

4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Mengaktifkan konfigurasi agen otomatis untuk akun anggota aktif yang ada

Manage for all Amazon ECS clusters (account level)

1. Pada halaman Runtime Monitoring, di bawah tab Konfigurasi, Anda dapat melihat status konfigurasi agen Otomatis saat ini.
2. Dalam panel konfigurasi agen otomatis, di bawah bagian Akun anggota aktif, pilih Tindakan.
3. Dari Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
4. Pilih Konfirmasi.
5. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS ini dengan pasangan nilai kunci sebagai -. `GuardDutyManaged` `false`
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
4. Di panel navigasi, pilih Runtime Monitoring.

5.
> **Note**
>
> Selalu tambahkan tag pengecualian ke kluster Amazon ECS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

   Di bawah tab Konfigurasi, di bagian Konfigurasi agen otomatis, di bawah Akun anggota aktif, pilih Tindakan.

6. Dari Tindakan, pilih Aktifkan untuk semua akun anggota aktif.

   Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

7. Pilih Konfirmasi.

8. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus `GuardDutyManaged` -. `true`

2. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Saat menggunakan tag inklusi untuk kluster Amazon ECS, Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan

Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
- UpdateServicedi Referensi API Layanan Amazon Elastic Container.
- update-service di Command Reference.AWS CLI

Auto-enable Konfigurasi agen otomatis untuk anggota baru

Manage for all Amazon ECS clusters (account level)

1. Pada halaman Runtime Monitoring, pilih Edit untuk memperbarui konfigurasi yang ada.
2. Di bagian Konfigurasi agen otomatis, pilih Aktifkan secara otomatis untuk akun anggota baru.
3. Pilih Simpan.
4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS ini dengan pasangan nilai kunci sebagai -. `GuardDutyManaged` `false`
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
4. Di panel navigasi, pilih Runtime Monitoring.
5.

> **Note**
>
> Selalu tambahkan tag pengecualian ke kluster Amazon ECS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

Di bawah tab Konfigurasi, pilih Aktifkan secara otomatis untuk akun anggota baru di bagian Konfigurasi agen otomatis.

Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

6. Pilih Simpan.
7. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus `GuardDutyManaged` -. `true`
2. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
```

```
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
```

```
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Saat menggunakan tag inklusi untuk kluster Amazon ECS, Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Mengaktifkan konfigurasi agen otomatis untuk akun anggota aktif secara selektif

Manage for all Amazon ECS (account level)

1. Pada halaman Akun, pilih akun yang ingin Anda aktifkan konfigurasi Monitoring-Automated agen Runtime (ECS-Fargate). Anda dapat memilih beberapa akun. Pastikan akun yang Anda pilih pada langkah ini sudah diaktifkan dengan Runtime Monitoring.
2. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi Monitoring-Automated agen Runtime (ECS-Fargate).
3. Pilih Konfirmasi.
4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS ini dengan pasangan nilai kunci sebagai -. `GuardDutyManaged` `false`
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

   JSON

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

```
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
```

```
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
4. Di panel navigasi, pilih Runtime Monitoring.
5.

> **Note**
>
> Selalu tambahkan tag pengecualian ke kluster Amazon ECS Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

   Pada halaman Akun, pilih akun yang ingin Anda aktifkan konfigurasi Monitoring-Automated agen Runtime (ECS-Fargate). Anda dapat memilih beberapa akun. Pastikan akun yang Anda pilih pada langkah ini sudah diaktifkan dengan Runtime Monitoring.

   Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

6. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi Monitoring-Automated agen Runtime (ECS-Fargate).
7. Pilih Simpan.
8. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Pastikan Anda tidak mengaktifkan konfigurasi agen Otomatis (atau konfigurasi agen Runtime Monitoring-Automated (ECS-Fargate)) untuk akun terpilih yang memiliki kluster Amazon ECS yang ingin Anda pantau.
2. Tambahkan tag ke cluster Amazon ECS yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus `GuardDutyManaged` -. `true`
3. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
```

```
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
```

```
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Saat menggunakan tag inklusi untuk kluster Amazon ECS, Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Mengkonfigurasi GuardDuty agen untuk akun mandiri

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi:

   a. Untuk mengelola konfigurasi agen otomatis untuk semua klaster Amazon ECS (tingkat akun)

      Pilih Aktifkan di bagian Konfigurasi agen otomatis untuk AWS Fargate (khusus ECS). Ketika tugas Fargate Amazon ECS baru diluncurkan, GuardDuty akan mengelola penyebaran agen keamanan.

      - Pilih Simpan.

   b. Untuk mengelola konfigurasi agen otomatis dengan mengecualikan beberapa klaster Amazon ECS (tingkat klaster)

      i. Tambahkan tag ke cluster Amazon ECS yang ingin Anda kecualikan semua tugasnya. Pasangan kunci-nilai harus `GuardDutyManaged` -. `false`

      ii. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

      JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
```

```
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn":
 "arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

iii. Di bawah tab Konfigurasi, pilih Aktifkan di bagian Konfigurasi agen otomatis.

> **Note**
>
> Selalu tambahkan tag pengecualian ke cluster Amazon ECS Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, agen keamanan akan digunakan di semua tugas yang diluncurkan dalam cluster Amazon ECS yang sesuai.

Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

iv. Pilih Simpan.

c. Untuk mengelola konfigurasi agen otomatis dengan menyertakan beberapa klaster Amazon ECS (tingkat klaster)

i. Tambahkan tag ke cluster Amazon ECS yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus `GuardDutyManaged` -. `true`

ii. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam Mencegah tag diubah kecuali oleh prinsip-prinsip resmi dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

JSON

```
{
```

```
   "Version":"2012-10-17",
   "Statement": [
       {
           "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
           "Effect": "Deny",
           "Action": [
               "ecs:TagResource",
               "ecs:UntagResource"
           ],
           "Resource": [
               "*"
           ],
           "Condition": {
               "StringNotEquals": {
                   "ecs:ResourceTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                   "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
               },
               "Null": {
                   "ecs:ResourceTag/GuardDutyManaged": false
               }
           }
       },
       {
           "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
           "Effect": "Deny",
           "Action": [
               "ecs:TagResource",
               "ecs:UntagResource"
           ],
           "Resource": [
               "*"
           ],
           "Condition": {
               "StringNotEquals": {
                   "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                   "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
               },
               "ForAnyValue:StringEquals": {
                   "aws:TagKeys": [
                       "GuardDutyManaged"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn":
 "arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan. `forceNewDeployment`

   Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

   - Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.
   - UpdateServicedi Referensi API Layanan Amazon Elastic Container.
   - update-service di Command Reference.AWS CLI

Mengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS

Runtime Monitoring mendukung pengaktifan agen keamanan melalui konfigurasi GuardDuty otomatis dan secara manual. Bagian ini menyediakan langkah-langkah untuk mengaktifkan konfigurasi agen otomatis untuk kluster Amazon EKS.

Sebelum melanjutkan, pastikan Anda telah mengikuti. Prasyarat untuk dukungan klaster Amazon EKS

Berdasarkan pendekatan pilihan Anda tentang cara melakukannyaKonfigurasi agen otomatis (disarankan), pilih langkah-langkah di bagian berikut yang sesuai.

Mengkonfigurasi agen otomatis untuk lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan konfigurasi agen otomatis untuk akun anggota, dan mengelola Agen otomatis untuk kluster EKS milik akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat Mengelola beberapa akun.

Mengkonfigurasi konfigurasi agen otomatis untuk akun administrator yang didelegasikan GuardDuty

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Jika Anda memilih Aktifkan untuk semua akun di bagian Runtime Monitoring, maka Anda memiliki opsi berikut: • Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua kluster EKS yang termasuk dalam akun akun GuardDuty administrator yang didelegasikan dan juga untuk semua kluster EKS yang termasuk dalam semua akun anggota yang ada dan berpotensi baru di organisasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	• Pilih Konfigurasikan akun secara manual. Jika Anda memilih Konfigurasi akun secara manual di bagian Runtime Monitoring, lakukan hal berikut: 1. Pilih Konfigurasi akun secara manual di bagian Konfigurasi agen otomatis. 2. Pilih Aktifkan di bagian akun GuardDuty administrator yang didelegasikan (akun ini). Pilih Simpan.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau semua kluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDuty Managed` dan nilainya sebagai`false`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* dengan`eks:TagResource` . • Ganti *ec2:DeleteTags* dengan`eks:UntagResource` . • Ganti *access-project* dengan `GuardDutyManaged` • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`Principal Arn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/. 4. Di panel navigasi, pilih Runtime Monitoring. **Note** Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. 5. Di bawah tab Konfigurasi, pilih Aktifkan di bagian manajemen GuardDuty agen. Untuk kluster EKS yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan. 6. Pilih Simpan. Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan telah digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDuty Managed` dan nilainya sebagai`false`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah

Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut:

- Ganti *ec2:CreateTags* denganeks:TagResource .
- Ganti *ec2:DeleteTags* denganeks:UntagResource .
- Ganti *access-project* dengan GuardDutyManaged
- Ganti *123456789012* dengan Akun AWS ID entitas tepercaya.

  Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipal Arn :

```
"aws:PrincipalArn":["arn:aws:iam::12345678901
2:role/org-admins/iam-admin", "arn:aws:iam::1234
56789012:role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/iam-admin"]
```

3. Jika Anda mengaktifkan agen otomatis untuk kluster EKS ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda.

   Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari klaster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring
4. Jika Anda mengelola agen GuardDuty keamanan untuk cluster EKS ini secara manual, lihatMenonaktifkan, menghapus instalasi , dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif menggunakan tag inklusi	Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau klaster EKS selektif di akun Anda: 1. Pastikan untuk memilih Nonaktifkan untuk akun GuardDuty administrator yang didelegasikan (akun ini) di bagian Konfigura si agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Tambahkan tag ke cluster EKS Anda dengan kunci as `GuardDutyManaged` dan nilainya sebagai`true`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *`ec2:CreateTags`* dengan`eks:TagResource` . • Ganti *`ec2:DeleteTags`* dengan`eks:UntagResource` . • Ganti *`access-project`* dengan `GuardDutyManaged` • Ganti *`123456789012`* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` :

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Mengelola agen GuardDuty keamanan secara manual	Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, Anda dapat mengelola agen keamanan secara manual untuk kluster EKS Anda. 1. Pastikan untuk memilih Nonaktifkan untuk akun GuardDuty administrator yang didelegasikan (akun ini) di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Auto-enable Agen otomatis untuk semua akun anggota

> **Note**
>
> Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Mengelola agen keamanan melalui GuardDuty	Topik ini adalah untuk mengaktifkan Runtime Monitoring untuk semua akun anggota dan oleh karena itu, langkah-langkah berikut mengasumsikan bahwa Anda harus memilih Aktifkan untuk semua akun di bagian Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
(Pantau semua kluster EKS)	1. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua kluster EKS yang termasuk dalam akun akun GuardDuty administrator yang didelegasikan dan juga untuk semua kluster EKS yang termasuk dalam semua akun anggota yang ada dan berpotensi baru di organisasi. 2. Pilih Simpan.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDuty Managed` dan nilainya sebagai`false`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* dengan`eks:TagResource` . • Ganti *ec2:DeleteTags* dengan`eks:UntagResource` . • Ganti *access-project* dengan `GuardDutyManaged` • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`Principal Arn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/. 4. Di panel navigasi, pilih Runtime Monitoring. **Note** Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan Agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. 5. Di bawah tab Konfigurasi, pilih Edit di bagian konfigurasi Runtime Monitoring. 6. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. Untuk kluster EKS yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan. 7. Pilih Simpan. Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan telah digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDuty Managed` dan nilainya sebagai`false`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Jika Anda mengaktifkan konfigurasi agen otomatis untuk kluster EKS ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya

terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda.

Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari klaster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring

3. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut:

   - Ganti *ec2:CreateTags* dengan`eks:TagResource` .
   - Ganti *ec2:DeleteTags* dengan`eks:UntagResource` .
   - Ganti *access-project* dengan `GuardDutyManaged`
   - Ganti *123456789012* dengan Akun AWS ID entitas tepercaya.

     Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`Principal Arn` :

     ```
     "aws:PrincipalArn":["arn:aws:iam::12345678901
     2:role/org-admins/iam-admin", "arn:aws:iam::1234
     56789012:role/org-admins/iam-admin", "arn:aws:
     iam::123456789012:role/org-admins/iam-admin"]
     ```

4. Jika Anda mengelola agen GuardDuty keamanan untuk cluster EKS ini secara manual, lihatMenonaktifkan, menghapus instalasi , dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau kluster EKS selektif menggunakan tag inklusi	Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau klaster EKS selektif untuk semua akun anggota di organisasi Anda: 1. Jangan aktifkan konfigurasi apa pun di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Tambahkan tag ke cluster EKS Anda dengan kunci as `GuardDutyManaged` dan nilainya sebagai`true`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *`ec2:CreateTags`* dengan`eks:TagResource` . • Ganti *`ec2:DeleteTags`* dengan`eks:UntagResource` . • Ganti *`access-project`* dengan `GuardDutyManaged` • Ganti *`123456789012`* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` :

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Mengelola agen GuardDuty keamanan secara manual	Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, Anda dapat mengelola agen keamanan secara manual untuk kluster EKS Anda. 1. Jangan aktifkan konfigurasi apa pun di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Mengaktifkan agen otomatis untuk semua akun anggota aktif yang ada

> **Note**
>
> Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Untuk mengelola agen GuardDuty keamanan untuk akun anggota aktif yang ada di organisasi Anda

- GuardDuty Untuk menerima acara runtime dari kluster EKS yang termasuk dalam akun anggota aktif yang ada di organisasi, Anda harus memilih pendekatan yang disukai untuk mengelola agen GuardDuty keamanan untuk kluster EKS ini. Untuk informasi lebih lanjut tentang masing-masing pendekatan ini, lihatMenyebarkan agen keamanan ke Amazon EKS.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Mengelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Untuk memantau semua klaster EKS untuk semua akun anggota aktif yang ada 1. Pada halaman Runtime Monitoring, di bawah tab Konfigurasi, Anda dapat melihat status konfigurasi agen Otomatis saat ini. 2. Dalam panel konfigurasi agen otomatis, di bawah bagian Akun anggota aktif, pilih Tindakan. 3. Dari Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada. 4. Pilih Konfirmasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDutyManaged` dan nilainya sebagai`false`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna. AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* dengan`eks:TagResource` . • Ganti *ec2:DeleteTags* dengan`eks:UntagResource` . • Ganti *access-project* dengan `GuardDutyManaged` • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` :

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya

```
"aws:PrincipalArn":["arn:aws:iam::12
3456789012:role/org-admins/iam-
admin", "arn:aws:iam::123456789012:
role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/ia
m-admin"]
```

3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
4. Di panel navigasi, pilih Runtime Monitoring.

> **Note**
>
> Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda.

5. Di bawah tab Konfigurasi, di panel konfigurasi agen otomatis, di bawah Akun anggota aktif, pilih Tindakan.
6. Dari Tindakan, pilih Aktifkan untuk semua akun anggota aktif.
7. Pilih Konfirmasi.

Untuk mengecualikan cluster EKS dari pemantauan setelah agen GuardDuty keamanan telah digunakan di cluster ini

1. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDutyManaged` dan nilainya sebagai`false`.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. Setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDuty Managed • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-``

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"] 3. Terlepas dari bagaimana Anda mengelola agen keamanan (melalui GuardDuty atau secara manual), untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari cluster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihatMenonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau kluster EKS selektif menggunakan tag inklusi	1. Pada halaman Akun, setelah Anda mengaktif kan Runtime Monitoring, jangan aktifkan Runtime Monitoring - Konfigurasi agen otomatis. 2. Tambahkan tag ke kluster EKS milik akun yang dipilih yang ingin Anda pantau. Pasangan kunci-nilai tag harus `GuardDutyManaged` -. `true` Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 3. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna. AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *`ec2:CreateTags`* dengan `eks:TagRe source` . • Ganti *`ec2:DeleteTags`* dengan `eks:Untag Resource` . • Ganti *`access-project`* dengan `GuardDuty Managed` • Ganti *`123456789012`* dengan Akun AWS ID entitas tepercaya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Mengelola agen GuardDuty keamanan secara manual	1. Pastikan Anda tidak memilih Aktifkan di bagian Konfigurasi agen otomatis. Tetap aktifkan Runtime Monitoring. 2. Pilih Simpan. 3. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Auto-enable konfigurasi agen otomatis untuk anggota baru

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Mengelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	1. Pada halaman Runtime Monitoring, pilih Edit untuk memperbarui konfigurasi yang ada. 2. Di bagian Konfigurasi agen otomatis, pilih Aktifkan secara otomatis untuk akun anggota baru. 3. Pilih Simpan.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDutyManaged` dan nilainya sebagai`false`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* dengan`eks:TagResource` . • Ganti *ec2:DeleteTags* dengan`eks:UntagResource` . • Ganti *access-project* dengan `GuardDutyManaged` • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya

```
", "arn:aws:iam::123456789012:role/org-
admins/iam-admin", "arn:aws:iam::1234
56789012:role/org-admins/iam-admin"]
```

3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
4. Di panel navigasi, pilih Runtime Monitoring.

> **Note**
>
> Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan konfigura si agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda.

5. Di bawah tab Konfigurasi, pilih Aktifkan secara otomatis untuk akun anggota baru di bagian manajemen GuardDuty agen.

   Untuk kluster EKS yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan.
6. Pilih Simpan.

Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan telah digunakan di cluster ini

1. Terlepas dari apakah Anda mengelola agen GuardDuty keamanan melalui GuardDuty atau secara manual, tambahkan tag ke cluster EKS ini dengan kunci as `GuardDutyManaged` dan nilainya sebagai`false`.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. Jika Anda mengaktifkan agen otomatis untuk kluster EKS ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda. Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari klaster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* dengan `eks:TagResource` . • Ganti *ec2:DeleteTags* dengan `eks:UntagResource` . • Ganti *access-project* dengan `GuardDuty Managed`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	• Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Jika Anda mengelola agen GuardDuty keamanan untuk cluster EKS ini secara manual, lihatMenonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau kluster EKS selektif menggunakan tag inklusi	Terlepas dari bagaimana Anda memilih untuk mengaktif kan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau klaster EKS selektif untuk akun anggota baru di organisasi Anda. 1. Pastikan untuk menghapus Aktifkan secara otomatis untuk akun anggota baru di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitorin g sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Tambahkan tag ke cluster EKS Anda dengan kunci as `GuardDutyManaged` dan nilainya sebagai`true`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* dengan`eks:TagRe source` . • Ganti *ec2:DeleteTags* dengan`eks:Untag Resource` .

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	• Ganti *access-project* dengan `GuardDuty Managed` • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Mengelola agen GuardDuty keamanan secara manual	Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, Anda dapat mengelola agen keamanan secara manual untuk kluster EKS Anda. 1. Pastikan kosongkan kotak centang Secara otomatis mengaktifkan akun anggota baru di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Mengkonfigurasi agen otomatis untuk akun anggota aktif secara selektif

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Mengelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	1. Pada halaman Akun, pilih akun yang ingin Anda aktifkan Konfigurasi agen otomatis. Anda dapat memilih lebih dari satu akun sekaligus. Pastikan akun yang Anda pilih pada langkah ini sudah mengaktifkan EKS Runtime Monitoring. 2. Dari paket Edit Protection pilih opsi yang sesuai untuk mengaktif kan Runtime Monitoring - Konfigurasi agen otomatis. 3. Pilih Konfirmasi.
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDuty Managed` dan nilainya sebagai`false`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya

Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`Principal Arn` :

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

> **Note**
>
> Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda.

4. Pada halaman Akun, pilih akun yang ingin Anda aktifkan Kelola agen secara otomatis. Anda dapat memilih lebih dari satu akun sekaligus.
5. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi Monitoring-Automated agen Runtime untuk akun yang dipilih.

   Untuk kluster EKS yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan.
6. Pilih Simpan.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan telah digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDuty Managed` dan nilainya sebagai`false`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. Jika sebelumnya Anda mengaktifkan konfigurasi agen otomatis untuk kluster EKS ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk klaster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda. Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari klaster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya

Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`Principal Arn` :

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

3. Jika Anda mengelola agen GuardDuty keamanan untuk cluster EKS ini secara manual, Anda harus menghapusnya. Untuk informasi selengkapnya, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau kluster EKS selektif menggunakan tag inklusi	Terlepas dari cara Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau klaster EKS selektif yang termasuk dalam akun yang dipilih: 1. Pastikan Anda tidak mengaktifkan konfigurasi Monitoring-Automated agen Runtime untuk akun terpilih yang memiliki kluster EKS yang ingin Anda pantau. 2. Tambahkan tag ke cluster EKS Anda dengan kunci as `GuardDutyManaged` dan nilainya sebagai`true`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. Setelah menambahkan tag, GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 3. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* dengan`eks:TagResource` . • Ganti *ec2:DeleteTags* dengan`eks:UntagResource` . • Ganti *access-project* dengan `GuardDutyManaged` • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` :

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Mengelola agen GuardDuty keamanan secara manual	1. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. Pastikan Anda tidak mengaktifkan Runtime Monitoring- Konfigurasi agen otomatis untuk salah satu akun yang dipilih. 2. Pilih Konfirmasi. 3. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Mengkonfigurasi agen otomatis untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun.

Setelah Anda mengaktifkan Runtime Monitoring, pastikan untuk menginstal agen GuardDuty keamanan melalui konfigurasi otomatis atau penerapan manual. Sebagai bagian dari menyelesaikan semua langkah yang tercantum dalam prosedur berikut, pastikan untuk menginstal agen keamanan.

Berdasarkan preferensi Anda untuk memantau semua atau sumber daya Amazon EKS selektif, pilih metode yang disukai dan ikuti langkah-langkah dalam tabel berikut.

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Runtime Monitoring.

3. Di bawah tab Konfigurasi, pilih Aktifkan untuk mengaktifkan konfigurasi agen otomatis untuk akun Anda.

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-langkahnya
Mengelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	1. Pilih Aktifkan di bagian Konfigurasi agen otomatis. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster EKS yang ada dan berpotensi baru di akun Anda. 2. Pilih Simpan.

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-langkahnya
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDutyManaged` dan nilainya sebagai`false`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna. AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* dengan`eks:TagResource` . • Ganti *ec2:DeleteTags* dengan`eks:UntagResource` . • Ganti *access-project* dengan `GuardDutyManaged` • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` :

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-langkahnya

```
"aws:PrincipalArn":["arn:aws:iam::12
3456789012:role/org-admins/iam-
admin", "arn:aws:iam::123456789012:
role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/ia
m-admin"]
```

3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
4. Di panel navigasi, pilih Runtime Monitoring.

> **Note**
>
> Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda.

5. Di bawah tab Konfigurasi, pilih Aktifkan di bagian manajemen GuardDuty agen.

   Untuk kluster EKS yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan.
6. Pilih Simpan.

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-langkahnya
	Untuk mengecualikan cluster EKS dari pemantauan setelah agen GuardDuty keamanan telah digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDutyManaged` dan nilainya sebagai`false`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. Setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna. AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *`ec2:CreateTags`* dengan`eks:TagResource` . • Ganti *`ec2:DeleteTags`* dengan`eks:UntagResource` . • Ganti *`access-project`* dengan `GuardDutyManaged`

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-langkahnya
	• Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari klaster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihatMenonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-langkahnya
Pantau kluster EKS selektif menggunakan tag inklusi	1. Pastikan untuk memilih Nonaktifkan di bagian Konfigurasi agen otomatis. Tetap aktifkan Runtime Monitoring. 2. Pilih Simpan. 3. Tambahkan tag ke cluster EKS ini dengan kunci as `GuardDutyManaged` dan nilainya sebagai`true`. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna. AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *`ec2:CreateTags`* dengan`eks:TagResource` . • Ganti *`ec2:DeleteTags`* dengan`eks:UntagResource` . • Ganti *`access-project`* dengan `GuardDutyManaged` • Ganti *`123456789012`* dengan Akun AWS ID entitas tepercaya.

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-langkahnya
	Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Kelola agen secara manual	1. Pastikan untuk memilih Nonaktifkan di bagian Konfigurasi agen otomatis. Tetap aktifkan Runtime Monitoring. 2. Pilih Simpan. 3. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Mengelola agen keamanan secara manual untuk klaster Amazon EKS

Bagian ini menjelaskan bagaimana Anda dapat mengelola agen add-on Amazon EKS (GuardDuty agen) setelah Anda mengaktifkan Runtime Monitoring (atau EKS Runtime Monitoring). Untuk menggunakan Runtime Monitoring, Anda harus mengaktifkan Runtime Monitoring dan mengonfigurasi add-on Amazon EKS,. `aws-guardduty-agent` Anda perlu melakukan kedua langkah GuardDuty untuk mendeteksi potensi ancaman dan menghasilkanGuardDuty Jenis penemuan Runtime Monitoring.

Untuk mengelola agen secara manual, Anda perlu membuat titik akhir VPC sebagai prasyarat. Ini membantu GuardDuty menerima acara runtime. Setelah ini, Anda dapat menginstal agen keamanan sehingga GuardDuty akan mulai menerima peristiwa runtime dari sumber daya Amazon EKS. Saat

GuardDuty merilis versi agen baru untuk sumber daya ini, Anda dapat memperbarui versi agen di akun Anda.

Topik

- Prasyarat - Membuat titik akhir VPC Amazon
- Menginstal agen GuardDuty keamanan secara manual di sumber daya Amazon EKS
- Memperbarui agen keamanan secara manual untuk sumber daya Amazon EKS

Prasyarat - Membuat titik akhir VPC Amazon

Sebelum Anda dapat menginstal agen GuardDuty keamanan, Anda harus membuat titik akhir Amazon Virtual Private Cloud (Amazon VPC). Ini akan membantu GuardDuty menerima peristiwa runtime dari sumber daya Amazon EKS Anda.

> **Note**
>
> Tidak ada biaya tambahan untuk penggunaan titik akhir VPC.

Pilih metode akses yang disukai untuk membuat titik akhir VPC Amazon.

Console

Untuk membuat titik akhir VPC

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, di bawah Virtual Private Cloud, pilih Endpoints.
3. Pilih Buat Titik Akhir.
4. Pada halaman Buat titik akhir, untuk kategori Layanan, pilih Layanan titik akhir lainnya.
5. Untuk nama Layanan, masukkan**`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

   Pastikan untuk mengganti *`us-east-1`* dengan Region yang benar. Ini harus Region yang sama dengan cluster EKS milik Akun AWS ID Anda.
6. Pilih Verifikasi layanan.
7. Setelah nama layanan berhasil diverifikasi, pilih VPC tempat klaster Anda berada. Tambahkan kebijakan berikut untuk membatasi penggunaan titik akhir VPC hanya ke akun tertentu. Dengan organisasi yang `Condition` disediakan di bawah kebijakan ini,

Anda dapat memperbarui kebijakan berikut untuk membatasi akses ke titik akhir Anda. Untuk memberikan dukungan titik akhir VPC ke ID akun tertentu di organisasi Anda, lihat. Organization condition to restrict access to your endpoint

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

ID `aws:PrincipalAccount` akun harus cocok dengan akun yang berisi titik akhir VPC dan VPC. Daftar berikut menunjukkan cara berbagi titik akhir VPC dengan ID lain: Akun AWS

Kondisi organisasi untuk membatasi akses ke titik akhir Anda

- Untuk menentukan beberapa akun untuk mengakses titik akhir VPC, ganti `"aws:PrincipalAccount": "111122223333"` dengan yang berikut:

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
```

```
    ]
```

- Untuk mengizinkan semua anggota dari organisasi mengakses titik akhir VPC, ganti `"aws:PrincipalAccount": "111122223333"` dengan yang berikut ini:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Untuk membatasi akses sumber daya ke ID organisasi, tambahkan `ResourceOrgID` ke kebijakan.

  Untuk informasi selengkapnya, lihat ResourceOrgID.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Di bawah Pengaturan tambahan, pilih Aktifkan nama DNS.
9. Di bawah Subnet, pilih subnet tempat klaster Anda berada.
10. Di bawah Grup keamanan, pilih grup keamanan yang mengaktifkan port 443 in-bound dari VPC Anda (atau kluster EKS Anda). Jika Anda belum memiliki grup keamanan yang mengaktifkan port 443 dalam terikat, Buat grup keamanan.

    Jika ada masalah saat membatasi izin masuk ke VPC (atau instance), Anda dapat menggunakan port 443 yang di-bound dari alamat IP apa pun. `(0.0.0.0/0)` Namun, GuardDuty rekomendasikan untuk menggunakan alamat IP yang cocok dengan blok CIDR untuk VPC Anda. Untuk informasi selengkapnya, lihat blok CIDR VPC di Panduan Pengguna Amazon VPC.

API/CLI

Untuk membuat titik akhir VPC

- Memohon. CreateVpcEndpoint
- Gunakan nilai berikut untuk parameter:
  - Untuk nama Layanan, masukkan**`com.amazonaws.us-east-1.guardduty-data`**.

    Pastikan untuk mengganti *`us-east-1`* dengan Region yang benar. Ini harus Region yang sama dengan cluster EKS milik Akun AWS ID Anda.
  - Untuk DNSOptions, aktifkan opsi DNS pribadi dengan menyetelnya ke. `true`
- Untuk AWS Command Line Interface, lihat create-vpc-endpoint.

Setelah Anda mengikuti langkah-langkahnya, lihat Memvalidasi konfigurasi titik akhir VPC untuk memastikan bahwa titik akhir VPC telah diatur dengan benar.

Menginstal agen GuardDuty keamanan secara manual di sumber daya Amazon EKS

Bagian ini menjelaskan bagaimana Anda dapat menyebarkan agen GuardDuty keamanan untuk pertama kalinya untuk kluster EKS tertentu. Sebelum Anda melanjutkan dengan bagian ini, pastikan Anda telah menyiapkan prasyarat dan mengaktifkan Runtime Monitoring untuk akun Anda. Agen GuardDuty keamanan (add-on EKS) tidak akan berfungsi jika Anda tidak mengaktifkan Runtime Monitoring.

Pilih metode akses pilihan Anda untuk menyebarkan agen GuardDuty keamanan untuk pertama kalinya.

Console

1. Buka konsol Amazon EKS di https://console.aws.amazon.com/eks/home#/cluster.
2. Pilih nama Cluster Anda.
3. Pilih Add-onstab.
4. Pilih Get more add-ons
5. Pada halaman Pilih add-on, pilih Amazon GuardDuty EKS Runtime Monitoring.
6. GuardDuty merekomendasikan memilih Versi agen terbaru dan default.
7. Pada halaman Konfigurasi pengaturan add-on yang dipilih, gunakan pengaturan default. Jika Status add-on EKS Anda Memerlukan aktivasi, pilih Aktifkan GuardDuty. Tindakan ini akan membuka GuardDuty konsol untuk mengonfigurasi Runtime Monitoring untuk akun Anda.
8. Setelah mengonfigurasi Runtime Monitoring untuk akun Anda, beralih kembali ke konsol Amazon EKS. Status add-on EKS Anda seharusnya telah berubah menjadi Siap untuk menginstal.
9. (Opsional) Menyediakan skema konfigurasi add-on EKS

   Untuk Versi add-on, jika Anda memilih v1.5.0 atau lebih tinggi, Runtime Monitoring mendukung konfigurasi parameter spesifik agen. GuardDuty Untuk informasi tentang rentang parameter, lihatKonfigurasikan parameter add-on EKS.

   a. Perluas Pengaturan konfigurasi opsional untuk melihat parameter yang dapat dikonfigurasi serta nilai serta format yang diharapkan.

b. Atur parameternya. Nilai-nilai harus dalam kisaran yang disediakan diKonfigurasikan parameter add-on EKS.

c. Pilih Simpan perubahan untuk membuat add-on berdasarkan konfigurasi lanjutan.

d. Untuk metode Resolusi konflik, opsi yang Anda pilih akan digunakan untuk menyelesaikan konflik saat Anda memperbarui nilai parameter ke nilai non-default. Untuk informasi selengkapnya tentang opsi yang tercantum, lihat ResolveConflicts di Referensi API Amazon EKS.

10. Pilih Berikutnya.
11. Pada halaman Tinjau dan buat, verifikasi semua detail, dan pilih Buat.
12. Arahkan kembali ke detail cluster dan pilih tab Resources.
13. Anda dapat melihat pod baru dengan awalan aws-guardduty-agent.

API/CLI

Anda dapat mengonfigurasi agen add-on Amazon EKS (`aws-guardduty-agent`) menggunakan salah satu opsi berikut:

- Jalankan CreateAddonuntuk akun Anda.
-

> **Note**
>
> Untuk add-on`version`, jika Anda memilih v1.5.0 atau lebih tinggi, Runtime Monitoring mendukung konfigurasi parameter spesifik agen. GuardDuty Untuk informasi selengkapnya, lihat Konfigurasikan parameter add-on EKS.

Gunakan nilai berikut untuk parameter permintaan:

- Untuk `addonName`, masukkan `aws-guardduty-agent`.

  Anda dapat menggunakan AWS CLI contoh berikut saat menggunakan nilai yang dapat dikonfigurasi yang didukung untuk versi add-on `v1.5.0` atau yang lebih baru. Pastikan untuk mengganti nilai placeholder yang disorot dengan warna merah dan yang terkait `Example.json` dengan nilai yang dikonfigurasi.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.17.1-eksbuild.2 --configuration-
values 'file://example.json'
```

Example.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

- Untuk informasi tentang didukung`addonVersion` , LihatVersi Kubernetes didukung oleh agen keamanan GuardDuty .
- Atau, Anda dapat menggunakan AWS CLI. Untuk informasi selengkapnya, lihat create-addon.

Nama DNS pribadi untuk titik akhir VPC

Secara default, agen keamanan menyelesaikan dan menghubungkan ke nama DNS pribadi dari titik akhir VPC. Untuk endpoint non-FIPS, DNS pribadi Anda akan muncul dalam format berikut:

Non-FIPS titik akhir — `guardduty-data.`*`us-east-1`*`.amazonaws.com`

Itu Wilayah AWS,*`us-east-1`*, akan berubah berdasarkan Wilayah Anda.

Memperbarui agen keamanan secara manual untuk sumber daya Amazon EKS

Ketika Anda mengelola agen GuardDuty keamanan secara manual, Anda bertanggung jawab untuk memperbaruinya untuk akun Anda. Untuk pemberitahuan tentang versi agen baru, Anda dapat berlangganan umpan RSS. GuardDuty versi rilis agen keamanan

Anda dapat memperbarui agen keamanan ke versi terbaru untuk mendapatkan manfaat dari dukungan dan peningkatan yang ditambahkan. Jika versi agen Anda saat ini mencapai akhir dukungan standar, maka untuk terus menggunakan Runtime Monitoring (atau EKS Runtime Monitoring), Anda harus memperbarui ke versi agen berikutnya yang tersedia atau terbaru.

Prasyarat

Sebelum Anda memperbarui versi agen keamanan, pastikan bahwa versi agen yang Anda rencanakan untuk digunakan sekarang, kompatibel dengan versi Kubernetes Anda. Untuk informasi selengkapnya, lihat Versi Kubernetes didukung oleh agen keamanan GuardDuty.

Console

1. Buka konsol Amazon EKS di https://console.aws.amazon.com/eks/home#/cluster.
2. Pilih nama Cluster Anda.
3. Di bawah Info cluster, pilih Add-onstab.
4. Di bawah Add-onstab, pilih GuardDutyEKS Runtime Monitoring.
5. Pilih Edit untuk memperbarui detail agen.
6. Pada halaman Configure GuardDuty EKS Runtime Monitoring, perbarui detailnya.
7. (Opsional) Memperbarui pengaturan konfigurasi opsional

   Jika versi add-on EKS Anda adalah 1.5.0 atau lebih tinggi, Anda juga dapat memperbarui skema konfigurasi add-on.

   a. Perluas pengaturan konfigurasi opsional untuk melihat skema konfigurasi.
   b. Perbarui nilai parameter berdasarkan rentang yang disediakan diKonfigurasikan parameter add-on EKS.
   c. Pilih Simpan perubahan untuk memulai pembaruan.
   d. Untuk metode Resolusi konflik, opsi yang Anda pilih akan digunakan untuk menyelesaikan konflik saat Anda memperbarui nilai parameter ke nilai non-default. Untuk informasi selengkapnya tentang opsi yang tercantum, lihat ResolveConflicts di Referensi API Amazon EKS.

API/CLI

Untuk memperbarui agen GuardDuty keamanan untuk kluster Amazon EKS Anda, lihat Memperbarui add-on.

> **Note**
>
> Untuk add-on`version`, jika Anda memilih 1.5.0 atau lebih tinggi, Runtime Monitoring mendukung konfigurasi parameter spesifik agen. GuardDuty Untuk informasi tentang rentang parameter, lihatKonfigurasikan parameter add-on EKS.

Anda dapat menggunakan AWS CLI contoh berikut saat menggunakan nilai yang dapat dikonfigurasi yang didukung untuk versi add-on 1.5.0 dan yang lebih baru. Pastikan untuk mengganti nilai placeholder yang disorot dengan warna merah dan yang terkait `Example.json` dengan nilai yang dikonfigurasi.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.17.1-eksbuild.2 --configuration-
values 'file://example.json'
```

Example.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Jika versi add-on Amazon EKS Anda 1.5.0 atau lebih tinggi, dan Anda telah mengonfigurasi skema add-on, Anda dapat memverifikasi apakah nilai muncul dengan benar untuk klaster Anda atau tidak. Untuk informasi selengkapnya, lihat Memverifikasi pembaruan skema konfigurasi.

Konfigurasikan parameter agen GuardDuty keamanan (add-on) untuk Amazon EKS

Anda dapat mengonfigurasi parameter spesifik agen GuardDuty keamanan Anda untuk Amazon EKS. Dukungan ini tersedia untuk agen GuardDuty keamanan versi 1.5.0 dan di atasnya. Untuk informasi tentang versi add-on terbaru, lihatGuardDuty versi agen keamanan untuk sumber daya Amazon EKS.

Mengapa saya harus memperbarui skema konfigurasi agen keamanan

> Skema konfigurasi untuk agen GuardDuty keamanan sama di semua kontainer dalam kluster Amazon EKS Anda. Jika nilai default tidak sejajar dengan beban kerja dan ukuran instans terkait, pertimbangkan untuk mengonfigurasi pengaturan CPU, pengaturan memori, dan pengaturan. `PriorityClass` `dnsPolicy` Terlepas dari bagaimana Anda mengelola GuardDuty agen untuk kluster Amazon EKS Anda, Anda dapat mengonfigurasi atau memperbarui konfigurasi parameter ini yang ada.

Perilaku konfigurasi agen otomatis dengan parameter yang dikonfigurasi

Ketika GuardDuty mengelola agen keamanan (EKS add-on) atas nama Anda, itu memperbarui add-on, sesuai kebutuhan. GuardDuty akan mengatur nilai parameter yang dapat dikonfigurasi ke nilai default. Namun, Anda masih dapat memperbarui parameter ke nilai yang diinginkan. Jika ini mengarah ke konflik, opsi default untuk ResolveConflicts adalah. `None`

Parameter dan nilai yang dapat dikonfigurasi

Untuk informasi tentang langkah-langkah untuk mengkonfigurasi parameter add-on, lihat:

- Menginstal agen GuardDuty keamanan secara manual di sumber daya Amazon EKS atau
- Memperbarui agen keamanan secara manual untuk sumber daya Amazon EKS

Tabel berikut menyediakan rentang dan nilai yang dapat Anda gunakan untuk menerapkan add-on Amazon EKS secara manual atau memperbarui pengaturan add-on yang ada.

Pengaturan CPU

Parameter	Nilai default	Rentang yang dapat dikonfigurasi
Permintaan	200m	Antara 200m dan 10000m, keduanya inklusif
Batas	1000m	Antara 200m dan 10000m, keduanya inklusif
`disableCpuLimits`	`false`	`true` atau `false`

`disableCpuLimits`Parameter ini tersedia untuk agen GuardDuty keamanan versi 1.12.1-eksbuild.3 dan yang lebih baru. Pada versi sebelumnya, add-on tidak mendukung parameter ini, dan API add-on Amazon EKS (`CreateAddon`,`UpdateAddon`) mengembalikan kesalahan validasi jika Anda menentukannya.

Saat Anda menyetel `disableCpuLimits` ke`true`, pod agen keamanan tidak memberlakukan batas CPU. Pengaturan sumber daya lainnya tidak terpengaruh.

Untuk menonaktifkan batas CPU, gunakan konfigurasi berikut:

```
{"resources":{"disableCpuLimits":true}}
```

Pengaturan memori

Parameter	Nilai default	Rentang yang dapat dikonfigurasi
Permintaan	256Mi	Antara 256Mi dan 20000Mi, keduanya inklusif
Batas	1024Mi	

PriorityClasspengaturan

Saat GuardDuty membuat add-on Amazon EKS untuk Anda, yang ditetapkan `PriorityClass` adalah`aws-guardduty-agent.priorityclass`. Ini berarti bahwa tidak ada tindakan yang akan diambil berdasarkan prioritas pod agen. Anda dapat mengonfigurasi parameter add-on ini dengan memilih salah satu `PriorityClass` opsi berikut:

Dapat dikonfigurasi **PriorityClass**	Nilai **preemptionPolicy**	**preemptionPolicy** deskripsi	Nilai pod
`aws-guardduty-agent.priorityclass`	`Never`	Tidak ada tindakan	1000000
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	Menetapkan nilai ini akan mendahului sebuah pod yang berjalan dengan nilai prioritas lebih rendah dari nilai pod agen.	100000000
`system-cluster-critical` [1]	`PreemptLowerPriority`		2000000000
`system-node-critical` [1]	`PreemptLowerPriority`		2000001000

[1] Kubernetes menyediakan dua `PriorityClass` opsi ini — dan. `system-cluster-critical` `system-node-critical` Untuk informasi selengkapnya, lihat PriorityClassdi dokumentasi Kubernetes.

dnsPolicypengaturan

Pilih salah satu opsi kebijakan DNS berikut yang didukung Kubernetes. Ketika tidak ada konfigurasi yang `ClusterFirst` ditentukan, digunakan sebagai nilai default.

- `ClusterFirst`
- `ClusterFirstWithHostNet`

- `Default`

Untuk informasi tentang kebijakan ini, lihat Kebijakan DNS Pod di dokumentasi Kubernetes.

Memverifikasi pembaruan skema konfigurasi

Setelah Anda mengonfigurasi parameter, lakukan langkah-langkah berikut untuk memverifikasi bahwa skema konfigurasi telah diperbarui:

1. Buka konsol Amazon EKS di https://console.aws.amazon.com/eks/home#/cluster.
2. Pada panel navigasi, silakan pilih Klaster.
3. Pada halaman Clusters, pilih nama Cluster yang ingin Anda verifikasi pembaruannya.
4. Pilih tab Sumber Daya.
5. Dari panel Jenis sumber daya, di bawah Beban kerja, pilih. DaemonSets
6. Pilih aws-guardduty-agent.
7. Pada halaman aws-guardduty-agent, pilih Tampilan mentah untuk melihat respons JSON yang belum diformat. Verifikasi bahwa parameter yang dapat dikonfigurasi menampilkan nilai yang Anda berikan.

Setelah Anda memverifikasi, beralih ke GuardDuty konsol. Pilih yang sesuai Wilayah AWS dan lihat status cakupan untuk kluster Amazon EKS Anda. Untuk informasi selengkapnya, lihat Cakupan runtime dan pemecahan masalah untuk klaster Amazon EKS.

Memvalidasi konfigurasi titik akhir VPC

Setelah Anda menginstal agen keamanan secara manual atau melalui konfigurasi GuardDuty otomatis, Anda dapat menggunakan dokumen ini untuk memvalidasi konfigurasi titik akhir VPC. Anda juga dapat menggunakan langkah-langkah ini setelah memecahkan masalah cakupan runtime untuk jenis sumber daya. Anda dapat memastikan bahwa langkah-langkah tersebut bekerja seperti yang diharapkan dan status cakupan berpotensi muncul sebagai Sehat.

Gunakan langkah-langkah berikut untuk memvalidasi bahwa konfigurasi titik akhir VPC untuk jenis sumber daya Anda diatur dengan benar di akun pemilik VPC:

1. Masuk ke Konsol Manajemen AWS dan buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/

2. Di panel navigasi, di bawah Virtual Private Cloud, pilih VPC Anda.
3. Pada halaman VPC Anda, pilih IPv4 CIDR yang terkait dengan ID VPC Anda.
4. Di panel navigasi, di bawah Virtual Private Cloud, pilih Endpoints.
5. Dalam tabel Endpoints, pilih baris yang memiliki nama Service mirip dengan com.amazonaws.***us-east-1***.guardduty-data. Region (`us-east-1`) mungkin berbeda untuk titik akhir Anda.
6. Panel untuk detail titik akhir akan muncul. Di bawah tab Grup Keamanan, pilih tautan ID Grup terkait untuk detail selengkapnya.
7. Dalam tabel Grup Keamanan, pilih baris dengan ID grup Keamanan terkait untuk melihat detailnya.
8. Di bawah tab Aturan masuk, pastikan bahwa ada kebijakan masuk dengan rentang Port sebagai 443 dan Sumber sebagai nilai yang disalin dari IPv4 CIDR. Aturan masuk mengontrol lalu lintas masuk yang diizinkan untuk mencapai instance. Gambar berikut menunjukkan aturan masuk untuk grup keamanan yang terkait dengan VPC yang digunakan oleh GuardDuty agen keamanan.

   Jika Anda belum memiliki grup keamanan yang mengaktifkan port masuk 443, Buat grup keamanan di Panduan Pengguna Amazon EC2.

   Jika ada masalah saat membatasi izin masuk ke VPC (atau cluster) Anda, izinkan lalu lintas masuk pada port 443 dari alamat IP apa pun (0.0.0. 0/0).

Daftar berikut mencakup item yang baik untuk diketahui setelah Anda menginstal atau memperbarui agen keamanan.

Menilai cakupan runtime

Langkah selanjutnya setelah menginstal atau memperbarui agen keamanan Anda adalah menilai cakupan runtime sumber daya Anda. Jika status cakupan runtime tidak sehat, maka Anda harus memecahkan masalah. Untuk informasi selengkapnya, lihat Masalah cakupan runtime dan pemecahan masalah.

Jika status cakupan runtime ditampilkan sebagai Sehat, ini menunjukkan bahwa Runtime Monitoring dapat mengumpulkan dan menerima peristiwa runtime. Untuk daftar acara ini, lihatJenis acara runtime yang dikumpulkan.

Nama DNS pribadi untuk titik akhir

Setelah Anda menginstal agen GuardDuty keamanan untuk sumber daya Anda, secara default, itu akan menyelesaikan dan terhubung ke nama DNS pribadi dari titik akhir VPC. Untuk endpoint non-FIPS, DNS pribadi akan muncul dalam format berikut:

`guardduty-data.`*`us-east-1`*`.amazonaws.com`

Itu Wilayah AWS,*`us-east-1`*, akan berubah berdasarkan Wilayah Anda.

Host dapat diinstal dengan dua agen keamanan

Saat bekerja dengan agen GuardDuty keamanan untuk instans Amazon EC2, Anda dapat menginstal dan menggunakan agen pada host yang mendasari dalam klaster Amazon EKS. Jika Anda telah menggunakan agen keamanan di cluster EKS itu, host yang sama dapat memiliki dua agen keamanan yang berjalan di dalamnya pada saat yang bersamaan. Untuk informasi tentang cara GuardDuty kerja dalam skenario ini, lihatAgen keamanan di host yang sama.

Meninjau statistik cakupan runtime dan masalah pemecahan masalah

Setelah Anda mengaktifkan Runtime Monitoring dan agen GuardDuty keamanan disebarkan ke sumber daya Anda, GuardDuty berikan statistik cakupan untuk jenis sumber daya yang sesuai dan status cakupan individual untuk sumber daya milik akun Anda. Status cakupan ditentukan dengan memastikan bahwa Anda telah mengaktifkan Runtime Monitoring, titik akhir VPC Amazon Anda telah dibuat, dan GuardDuty agen keamanan untuk sumber daya terkait telah digunakan. Status cakupan Sehat menunjukkan bahwa ketika ada peristiwa runtime yang terkait dengan sumber daya Anda, GuardDuty dapat menerima peristiwa runtime tersebut melalui titik akhir VPC Amazon, dan memantau perilakunya. Jika ada masalah pada saat mengonfigurasi Runtime Monitoring, membuat endpoint Amazon VPC, atau menerapkan agen GuardDuty keamanan, status cakupan akan muncul sebagai Tidak Sehat. Jika status cakupan tidak sehat, tidak GuardDuty akan dapat menerima atau memantau perilaku runtime sumber daya yang sesuai, atau menghasilkan temuan Runtime Monitoring.

Topik berikut akan membantu Anda meninjau statistik cakupan, mengonfigurasi EventBridge notifikasi, dan memecahkan masalah cakupan untuk jenis sumber daya tertentu.

Daftar Isi

- Cakupan runtime dan pemecahan masalah untuk instans Amazon EC2
- Cakupan runtime dan pemecahan masalah untuk Bottlerocket ECS-EC2
- Cakupan runtime dan pemecahan masalah untuk klaster Amazon ECS
- Cakupan runtime dan pemecahan masalah untuk klaster Amazon EKS

Cakupan runtime dan pemecahan masalah untuk instans Amazon EC2

Untuk sumber daya Amazon EC2, cakupan runtime dievaluasi pada tingkat instans. Instans Amazon EC2 Anda dapat menjalankan beberapa jenis aplikasi dan beban kerja antara lain di lingkungan Anda. AWS Fitur ini juga mendukung instans Amazon EC2 yang dikelola Amazon ECS dan jika Anda memiliki cluster Amazon ECS yang berjalan pada instans Amazon EC2, masalah cakupan pada tingkat instans akan muncul di bawah cakupan runtime Amazon EC2.

Topik

- Meninjau statistik cakupan
- Perubahan status cakupan dengan EventBridge notifikasi
- Memecahkan masalah cakupan runtime Amazon EC2

Meninjau statistik cakupan

Statistik cakupan untuk instans Amazon EC2 yang terkait dengan akun Anda sendiri atau akun anggota Anda adalah persentase instans EC2 yang sehat di semua instans EC2 yang dipilih. Wilayah AWS Persamaan berikut mewakili ini sebagai:

(instances/All Contoh sehat) * 100

Jika Anda juga telah menerapkan agen GuardDuty keamanan untuk kluster Amazon ECS, maka masalah cakupan tingkat instans apa pun yang terkait dengan kluster Amazon ECS yang berjalan di instans Amazon EC2 akan muncul sebagai masalah cakupan runtime instans Amazon EC2.

Pilih salah satu metode akses untuk meninjau statistik cakupan akun Anda.

Console

- Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

- Di panel navigasi, pilih Runtime Monitoring.
- Pilih tab cakupan Runtime.
- Di bawah tab cakupan runtime instans EC2, Anda dapat melihat statistik cakupan yang dikumpulkan berdasarkan status cakupan setiap instans Amazon EC2 yang tersedia di tabel daftar Instans.
  - Anda dapat memfilter tabel daftar Instance dengan kolom berikut:
    - ID Akun
    - Jenis manajemen agen
    - Versi agen
    - Status cakupan
    - ID Instance
    - Kluster ARN
- Jika salah satu instans EC2 Anda memiliki status Cakupan sebagai Tidak Sehat, kolom Masalah mencakup informasi tambahan tentang alasan status Tidak Sehat.

API/CLI

- Jalankan ListCoverageAPI dengan ID detektor valid Anda sendiri, Wilayah saat ini, dan titik akhir layanan. Anda dapat memfilter dan mengurutkan daftar instance menggunakan API ini.
  - Anda dapat mengubah contoh `filter-criteria` dengan salah satu opsi berikut untuk`CriterionKey`:
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `AGENT_VERSION`
    - `MANAGEMENT_TYPE`
    - `INSTANCE_ID`
    - `CLUSTER_ARN`
  - Saat `filter-criteria` disertakan `RESOURCE_TYPE` sebagai EC2, Runtime Monitoring tidak mendukung penggunaan ISSUE sebagai. `AttributeName` Jika Anda menggunakannya, respons API akan menghasilkan`InvalidInputException`.
  - Anda dapat mengubah contoh `AttributeName` `sort-criteria` dengan opsi berikut:

    - ACCOUNT_ID
    - COVERAGE_STATUS
    - INSTANCE_ID
    - UPDATED_AT
  - Anda dapat mengubah *max-results* (hingga 50).
  - Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. detectorId

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Jalankan GetCoverageStatisticsAPI untuk mengambil statistik agregat cakupan berdasarkan. statisticsType
  - Anda dapat mengubah contoh statisticsType ke salah satu opsi berikut:
    - COUNT_BY_COVERAGE_STATUS— Merupakan statistik cakupan untuk kluster EKS yang dikumpulkan berdasarkan status cakupan.
    - COUNT_BY_RESOURCE_TYPE— Statistik cakupan dikumpulkan berdasarkan jenis AWS sumber daya dalam daftar.
    - Anda dapat mengubah contoh filter-criteria dalam perintah. Anda dapat menggunakan opsi berikut untukCriterionKey:
      - ACCOUNT_ID
      - RESOURCE_TYPE
      - COVERAGE_STATUS
      - AGENT_VERSION
      - MANAGEMENT_TYPE
      - INSTANCE_ID
      - CLUSTER_ARN
  - Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. detectorId

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Jika status cakupan instans EC2 Anda tidak sehat, lihatMemecahkan masalah cakupan runtime Amazon EC2.

Perubahan status cakupan dengan EventBridge notifikasi

Status cakupan instans Amazon EC2 Anda mungkin tampak tidak sehat. Untuk mengetahui kapan status pertanggungan berubah, kami sarankan Anda untuk memantau status pertanggungan secara berkala, dan memecahkan masalah jika status menjadi tidak sehat. Atau, Anda dapat membuat EventBridge aturan Amazon untuk menerima pemberitahuan saat status cakupan berubah dari Tidak Sehat menjadi Sehat atau lainnya. Secara default, GuardDuty publikasikan ini di EventBridge bus untuk akun Anda.

Skema pemberitahuan sampel

Dalam EventBridge aturan, Anda dapat menggunakan contoh peristiwa dan pola peristiwa yang telah ditentukan sebelumnya untuk menerima pemberitahuan status cakupan. Untuk informasi selengkapnya tentang membuat EventBridge aturan, lihat Membuat aturan di Panduan EventBridge Pengguna Amazon.

Selain itu, Anda dapat membuat pola acara khusus dengan menggunakan skema pemberitahuan contoh berikut. Pastikan untuk mengganti nilai untuk akun Anda. Untuk mendapatkan pemberitahuan saat status cakupan instans Amazon EC2 Anda berubah `Healthy` dari `Unhealthy` ke, seharusnya begitu`detail-type`. *`GuardDuty Runtime Protection Unhealthy`* Untuk mendapatkan pemberitahuan ketika status cakupan berubah dari `Unhealthy` ke`Healthy`, ganti nilai `detail-type` dengan*`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Akun AWS ID",
  "time": "event timestamp (string)",
```

```
  "region": "Wilayah AWS",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EC2",
        "ec2InstanceDetails": {
          "instanceId":"",
          "instanceType":"",
          "clusterArn": "",
          "agentDetails": {
            "version":""
          },
          "managementType":""
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Memecahkan masalah cakupan runtime Amazon EC2

Jika status cakupan instans Amazon EC2 Anda tidak sehat, Anda dapat melihat alasannya di bawah kolom Masalah.

Jika instans EC2 Anda dikaitkan dengan kluster EKS dan agen keamanan untuk EKS diinstal baik secara manual atau melalui konfigurasi agen otomatis, lalu untuk memecahkan masalah cakupan, lihat. Cakupan runtime dan pemecahan masalah untuk klaster Amazon EKS

Tabel berikut mencantumkan jenis masalah dan langkah pemecahan masalah yang sesuai.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Tidak Ada Pelaporan Agen	Menunggu notifikasi SSM	Menerima pemberitahuan SSM mungkin memakan waktu beberapa menit.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
		Pastikan instans Amazon EC2 dikelola SSM. Untuk informasi selengkapnya, lihat langkah-langkah di bawah Metode 1 - Dengan menggunakan AWS Systems Manager diMemasang agen keamanan secara manual.
	(Kosong dengan sengaja)	Jika Anda mengelola agen GuardDuty keamanan secara manual, pastikan Anda mengikuti langkah-langkah di bawah iniMengelola agen keamanan secara manual untuk sumber daya Amazon EC2.
		Jika Anda telah mengaktifkan konfigurasi agen otomatis: • Instans EC2 Anda dikelola SSM. • Lihat status agen keamanan Anda secara berkala. Untuk informasi selengkapnya, lihat Memvalidasi status instalasi agen GuardDuty keamanan.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
		Validasi bahwa titik akhir VPC untuk instans Amazon EC2 Anda telah dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat Memvalidasi konfigurasi titik akhir VPC.
		Jika organisasi Anda memiliki kebijakan kontrol layanan (SCP), validasi bahwa batas izin tidak membatasi izin. `guardduty:SendSecurityTelemetry` Untuk informasi selengkapnya, lihat Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
	Agen terputus	• Lihat status agen keamanan Anda. Untuk informasi selengkapnya, lihat Memvalidasi status instalasi agen GuardDuty keamanan. • Lihat log agen keamanan untuk mengidentifikasi akar penyebab potensial. Log memberikan kesalahan terperinci yang dapat Anda gunakan untuk memecahkan masalah sendiri. File log tersedia di bawah `/var/log/amzn-guardduty-agent/` . Lakukan `sudo journalctl -u amazon-guardduty-agent` .
Agen Tidak Disediakan	Instance dengan tag pengecualian dikecualikan dari Runtime Monitoring.	GuardDuty tidak menerima peristiwa runtime dari instans Amazon EC2 yang diluncurkan dengan tag pengecualian:. `GuardDutyManaged false` Untuk menerima peristiwa runtime dari instans Amazon EC2 ini, hapus tag pengecualian.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
	Versi kernel lebih rendah dari versi yang didukung.	Untuk informasi tentang versi kernel yang didukung di seluruh distribusi OS, lihat Validasi persyaratan arsitektur instans Amazon EC2.
	Versi kernel lebih tinggi dari versi yang didukung.	Untuk informasi tentang versi kernel yang didukung di seluruh distribusi OS, lihat Validasi persyaratan arsitektur instans Amazon EC2.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
	Tidak dapat mengambil dokumen identitas instance.	Ikuti langkah-langkah ini: 1. Konfirmasikan bahwa sumber daya Anda adalah instans Amazon EC2, dan bukan instance non-EC2 hybrid. 2. Konfirmasikan bahwa Layanan Metadata Instans (IMDS) diaktifkan. Untuk melakukannya, lihat Mengonfigurasi opsi Layanan Metadata Instance di Panduan Pengguna Amazon EC2. 3. Verifikasi bahwa dokumen identitas instance ada. Untuk melakukannya, lihat Mengambil dokumen identitas instans di Panduan Pengguna Amazon EC2. 4. Jika dokumen identitas instance masih belum ada, maka restart instance. Dokumen identitas instans dibuat saat instans dihentikan dan dimulai, dimulai ulang, atau diluncurkan.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Pembuatan Asosiasi SSM Gagal	GuardDuty Asosiasi SSM sudah ada di akun Anda	1. Hapus asosiasi yang ada secara manual. Untuk informasi selengkapnya, lihat Menghapus asosiasi di Panduan AWS Systems Manager Pengguna. 2. Setelah Anda menghapus asosiasi, nonaktifkan lalu aktifkan kembali konfigura si agen GuardDuty otomatis untuk Amazon EC2.
	Akun Anda memiliki terlalu banyak asosiasi SSM	Pilih salah satu dari dua opsi berikut: • Hapus asosiasi SSM yang tidak digunakan. Untuk informasi selengkapnya, lihat Menghapus asosiasi di Panduan AWS Systems Manager Pengguna. • Periksa apakah akun Anda memenuhi syarat untuk kenaikan kuota. Untuk informasi selengkap nya, lihat kuota Layanan Systems Manager di bagian. Referensi Umum AWS
Pembaruan Asosiasi SSM Gagal	GuardDuty Asosiasi SSM tidak ada di akun Anda	GuardDuty Asosiasi SSM tidak ada di akun Anda. Nonaktifk an dan kemudian aktifkan kembali Runtime Monitoring.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Penghapusan Asosiasi SSM Gagal	GuardDuty Asosiasi SSM tidak ada di akun Anda	Asosiasi SSM tidak ada di akun Anda. Jika asosiasi SSM dihapus dengan sengaja, maka tidak ada tindakan yang diperlukan.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Eksekusi Asosiasi Instans SSM Gagal	Persyaratan arsitektur atau prasyarat lainnya tidak terpenuhi.	Untuk informasi tentang distribusi sistem operasi terverifikasi, lihatPrasyarat untuk dukungan instans Amazon EC2. Jika Anda masih mengalami masalah ini, langkah-langkah berikut akan membantu Anda mengidentifikasi dan berpotensi menyelesaikan masalah: 1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/. 2. Di panel navigasi, di bawah Manajemen node, pilih Manajer Negara. 3. Filter berdasarkan properti Nama Dokumen dan masukkan AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Pilih ID asosiasi yang sesuai dan lihat riwayat Eksekusinya. 5. Menggunakan riwayat eksekusi, melihat kegagalan, mengidentifikasi akar penyebab

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
		potensial, dan mencoba untuk menyelesaikannya.
Pembuatan Titik Akhir VPC Gagal	Pembuatan titik akhir VPC tidak didukung untuk VPC bersama *vpcId*	Runtime Monitoring mendukung penggunaan VPC bersama dalam suatu organisasi. Untuk informasi selengkapnya, lihat Menggunakan VPC bersama dengan Runtime Monitoring.
	Hanya saat menggunakan VPC bersama dengan konfigurasi agen otomatis ID akun pemilik *111122223333* untuk VPC bersama *vpcId* tidak mengaktifkan Runtime Monitoring, konfigurasi agen otomatis, atau keduanya	Akun pemilik VPC bersama harus mengaktifkan Runtime Monitoring dan konfigurasi agen otomatis untuk setidaknya satu jenis sumber daya (Amazon EKS atau Amazon ECS ()).AWS Fargate Untuk informasi selengkapnya, lihat Prasyarat khusus untuk Runtime Monitoring GuardDuty.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
	Mengaktifkan DNS pribadi memerlukan atribut keduanya dan `enableDnsSupport` `enableDnsHostnames` VPC disetel ke `true` for *`vpcId`* (Layanan: Ec2, Status Code:400, ID Permintaan:). *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*	Pastikan atribut VPC berikut disetel ke `true` — `enableDnsSupport` dan. `enableDnsHostnames` Untuk informasi selengkapnya, lihat atribut DNS di VPC Anda. Jika Anda menggunakan Konsol VPC Amazon di https://console.aws.amazon.com/vpc/untuk membuat VPC Amazon, pilih Aktifkan nama host DNS dan Aktifkan resolusi DNS. Untuk informasi selengkapnya, lihat opsi konfigurasi VPC. Setelah memperbarui atribut VPC, Anda harus mempercepat percobaan ulang pembuatan titik akhir VPC dengan membuat salah satu perubahan ini: • Anda dapat menambahkan atau memodifikasi `GuardDutyManaged` tag untuk instans Amazon EC2 Anda (disarankan). Misalnya, Anda dapat menambahkan`GuardDutyManaged` : `true` untuk menyertakan instance untuk Runtime Monitoring.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
		• Anda dapat mengubah status instans Amazon EC2 (berhenti atau mulai ulang).
Penghapusan Titik Akhir VPC Bersama Gagal	Penghapusan titik akhir VPC bersama tidak diizinkan untuk ID akun, VPC *111122223333* bersama, ID akun pemilik. *vpcId 555555555555*	Langkah-langkah potensial: • Menonaktifkan status Pemantauan Waktu Proses akun peserta VPC bersama tidak memengaruhi kebijakan titik akhir VPC bersama dan grup keamanan yang ada di akun pemilik. Untuk menghapus titik akhir VPC bersama dan grup keamanan, Anda harus menonaktifkan Pemantauan Waktu Proses atau status konfigurasi agen otomatis di akun pemilik VPC bersama. • Akun peserta VPC bersama tidak dapat menghapus titik akhir VPC bersama dan grup keamanan yang dihosting di akun pemilik VPC bersama.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Agen tidak melaporkan	(Kosong dengan sengaja)	Jenis masalah telah mencapai akhir dukungan. Jika Anda terus mengalami masalah ini dan belum melakukannya, aktifkan agen GuardDuty otomatis untuk Amazon EC2. Jika masalah masih berlanjut , pertimbangkan untuk menonaktifkan Runtime Monitoring selama beberapa menit dan kemudian aktifkan lagi.

Cakupan runtime dan pemecahan masalah untuk Bottlerocket ECS-EC2

Untuk instans Amazon EC2 Bottlerocket di klaster GuardDuty Amazon ECS, evaluasi cakupan runtime di tingkat instans. Agen GuardDuty keamanan berjalan sebagai wadah host di Bottlerocket, bukan sebagai paket RPM atau Debian yang diinstal.

Instans Amazon EC2 Bottlerocket muncul di bawah tab cakupan runtime instans EC2. Untuk meninjau statistik cakupan instans Bottlerocket Anda, buka GuardDuty konsol, pilih Runtime Monitoring di panel navigasi, lalu pilih tab cakupan Runtime. Di bawah cakupan runtime instans EC2, Anda dapat melihat status cakupan setiap instans dan memfilter berdasarkan ID akun, versi agen, atau status cakupan. Untuk informasi selengkapnya, lihat Meninjau statistik cakupan.

Memecahkan masalah cakupan runtime Bottlerocket ECS-EC2

Jika status cakupan instans Amazon EC2 Bottlerocket Anda tidak sehat, Anda dapat melihat alasannya di bawah kolom Masalah.

Tabel berikut mencantumkan jenis masalah dan langkah pemecahan masalah yang sesuai.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Tidak Ada Pelaporan Agen	Menunggu notifikasi SSM	Menerima pemberitahuan SSM mungkin memakan waktu beberapa menit. Pastikan instans Bottleroc ket Anda dikelola SSM. Agen SSM berjalan di wadah kontrol Bottlerocket secara default. Verifikasi bahwa profil instans menyertakan `AmazonSSM ManagedInstanceCor e` dan kebijakan `AmazonEC2 ContainerRegistryR eadOnly` terkelola.
Tidak Ada Pelaporan Agen	Tidak berlaku	Verifikasi bahwa wadah host agen diaktifkan dan dijalanka n: 1. Connect ke instans Anda menggunakan SSM Session Manager. 2. Masukkan wadah admin:`enter-admin- container` . 3. Verifikasi pengatura n:`apiclient get settings.host-cont ainers.amazon- guardduty-agent` . Konfirmasikan itu `enabled` `superpowered` adalah `true` dan sedang`true`.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
		4. Periksa apakah proses agen sedang berjalan: `sheltie ps aux | grep guardduty .` 5. Periksa log agen menggunakan salah satu dari berikut ini: • `sheltie journalctl -u host-containers@amazon-guardduty-agent` • Dari sesi sheltie (`sudo sheltie`):`ls /var/log/amzn-guardduty-agent/ .`
Tidak Ada Pelaporan Agen	Tidak berlaku	Validasi bahwa instans memiliki konektivitas jaringan ke titik akhir Amazon ECR dan titik akhir GuardDuty VPC. Jika instans Anda berjalan di subnet pribadi, pastikan Anda telah mengonfigurasi titik akhir VPC untuk Amazon ECR dan. GuardDuty
Tidak Ada Pelaporan Agen	Tidak berlaku	Jika organisasi Anda memiliki kebijakan kontrol layanan (SCP), konfirmasikan bahwa batas izin mengizinkan izin tersebut. `guardduty:SendSecurityTelemetry`

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Pembuatan Asosiasi SSM Gagal	GuardDuty Asosiasi SSM sudah ada di akun Anda.	1. Hapus asosiasi yang ada secara manual. Untuk informasi selengkapnya, lihat Menghapus asosiasi di Panduan AWS Systems Manager Pengguna. 2. Setelah Anda menghapus asosiasi, nonaktifkan lalu aktifkan kembali konfigura si agen GuardDuty otomatis untuk Amazon EC2.
Pembuatan Asosiasi SSM Gagal	Akun Anda memiliki terlalu banyak asosiasi SSM.	Pilih salah satu dari dua opsi berikut: • Hapus asosiasi SSM yang tidak digunakan. Untuk informasi selengkapnya, lihat Menghapus asosiasi di Panduan AWS Systems Manager Pengguna. • Periksa apakah akun Anda memenuhi syarat untuk kenaikan kuota. Untuk informasi selengkap nya, lihat kuota Layanan Systems Manager di bagian. Referensi Umum AWS
Pembaruan Asosiasi SSM Gagal	GuardDuty Asosiasi SSM tidak ada di akun Anda.	GuardDuty Asosiasi SSM tidak ada di akun Anda. Nonaktifk an dan kemudian aktifkan kembali Runtime Monitoring.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Penghapusan Asosiasi SSM Gagal	GuardDuty Asosiasi SSM tidak ada di akun Anda.	Asosiasi SSM tidak ada di akun Anda. Jika asosiasi SSM dihapus dengan sengaja, maka tidak ada tindakan yang diperlukan.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Eksekusi Asosiasi Instans SSM Gagal	Persyaratan arsitektur atau prasyarat lainnya tidak terpenuhi.	Untuk informasi tentang persyaratan terverifikasi, lihatPrasyarat untuk dukungan Bottlerocket ECS-EC2. Jika Anda masih mengalami masalah ini, periksa riwayat eksekusi SSM State Manager: 1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/. 2. Di panel navigasi, di bawah Manajemen node, pilih Manajer Negara. 3. Filter berdasarkan properti Nama Dokumen dan masukkan AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Pilih ID asosiasi yang sesuai dan lihat riwayat Eksekusinya. 5. Menggunakan riwayat eksekusi, melihat kegagalan, mengidentifikasi akar penyebab potensial, dan mencoba untuk menyelesaikannya.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Agen terputus	Tidak berlaku	• Periksa log agen dari wadah admin: `enter-admin-container sheltie journalctl -u host-containers@amazon-guardduty-agent` • Pastikan image kontainer agen berhasil ditarik dengan memeriksa apakah `source` bidang dalam pengaturan penampung host mengarah ke URI ECR Amazon yang valid. • Pastikan profil instance memiliki izin tarik Amazon ECR. Untuk informasi selengkapnya, lihat Jadikan instans EC2 SSM dikelola dan konfigurasikan izin instans.
Agen Tidak Disediakan	Instance dengan tag pengecualian dikecualikan dari Runtime Monitoring.	GuardDuty tidak menerima peristiwa runtime dari instans Amazon EC2 yang diluncurkan dengan tag pengecualian:. `GuardDutyManaged false` Untuk menerima peristiwa runtime dari instance ini, hapus tag pengecualian.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Agen Tidak Disediakan	Versi kernel lebih rendah dari versi yang didukung.	Perbarui ke Bottlerocket terbaru atau ECS-3 AMI yang ECS-2 dioptimalkan atau yang lebih baru untuk `v1.62.1` konfigurasi agen otomatis.
Tarik Gambar ECR Gagal	Gambar wadah agen tidak dapat ditarik dari Amazon ECR.	• Verifikasi profil instans menyertakan kebijakan `AmazonEC2ContainerRegistryReadOnly` terkelola atau izin ECR Amazon individual yang diperlukan. • Verifikasi konektivitas jaringan ke titik akhir Amazon ECR di Wilayah Anda. • Jika menggunakan subnet pribadi, pastikan titik akhir VPC dikonfigurasi. Untuk informasi selengkapnya, lihat Persyaratan konektivitas jaringan.

Cakupan runtime dan pemecahan masalah untuk klaster Amazon ECS

Cakupan runtime untuk klaster Amazon ECS mencakup tugas yang sedang berjalan dan instans penampung AWS Fargate Amazon ECS. [1]

Untuk klaster Amazon ECS yang berjalan di Fargate, cakupan runtime dinilai pada tingkat tugas. Cakupan runtime cluster ECS mencakup tugas-tugas Fargate yang sudah mulai berjalan setelah Anda mengaktifkan Runtime Monitoring dan konfigurasi agen otomatis untuk Fargate (hanya ECS). Secara default, tugas Fargate tidak dapat diubah. GuardDuty tidak akan dapat menginstal agen keamanan untuk memantau kontainer pada tugas yang sudah berjalan. Untuk memasukkan tugas

Fargate seperti itu, Anda harus berhenti dan memulai tugas lagi. Pastikan untuk memeriksa apakah layanan terkait didukung.

Untuk informasi tentang wadah Amazon ECS, lihat Pembuatan kapasitas.

Daftar Isi

- Meninjau statistik cakupan
- Perubahan status cakupan dengan EventBridge notifikasi
- Memecahkan masalah cakupan ECS-Fargate runtime Amazon

Meninjau statistik cakupan

Statistik cakupan untuk sumber daya Amazon ECS yang terkait dengan akun Anda sendiri atau akun anggota Anda adalah persentase klaster Amazon ECS yang sehat di semua cluster Amazon ECS yang dipilih. Wilayah AWS Ini termasuk cakupan untuk cluster Amazon ECS yang terkait dengan instans Fargate dan Amazon EC2. Persamaan berikut mewakili ini sebagai:

(clusters/All Cluster sehat) * 100

Pertimbangan-pertimbangan

- Statistik cakupan untuk cluster ECS mencakup status cakupan tugas Fargate atau instance kontainer ECS yang terkait dengan cluster ECS tersebut. Status cakupan tugas Fargate mencakup tugas yang berada dalam status berjalan atau baru saja selesai berjalan.
- Di tab cakupan runtime cluster ECS, bidang yang dicakup instans Container menunjukkan status cakupan instans container Amazon EC2 yang terkait dengan cluster Amazon ECS Anda.

  Jika klaster Amazon ECS Anda hanya menjalankan jenis peluncuran Fargate, bidang ini menampilkan tanda hubung (-) untuk menunjukkan bahwa jumlah tersebut tidak berlaku. Fargate-only Cluster tidak memiliki instans penampung Amazon EC2 untuk dicakup.
- Jika klaster Amazon ECS Anda dikaitkan dengan instans Amazon EC2 yang tidak memiliki agen keamanan, klaster Amazon ECS juga akan memiliki status cakupan Tidak Sehat.

  Untuk mengidentifikasi dan memecahkan masalah cakupan untuk instans Amazon EC2 terkait, lihat instans Memecahkan masalah cakupan runtime Amazon EC2 Amazon EC2.

Pilih salah satu metode akses untuk meninjau statistik cakupan akun Anda.

Console

- Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
- Di panel navigasi, pilih Runtime Monitoring.
- Pilih tab cakupan Runtime.
- Di bawah tab cakupan runtime cluster ECS, Anda dapat melihat statistik cakupan yang dikumpulkan berdasarkan status cakupan setiap klaster Amazon ECS yang tersedia di tabel daftar Clusters.
  - Anda dapat memfilter tabel daftar Cluster dengan kolom berikut:
    - ID Akun
    - Nama Cluster
    - Jenis manajemen agen
    - Status cakupan
- Jika salah satu cluster Amazon ECS Anda memiliki status Cakupan sebagai Tidak Sehat, kolom Masalah menyertakan informasi tambahan tentang alasan status Tidak Sehat.

  Jika cluster Amazon ECS dikaitkan dengan instans Amazon EC2, navigasikan ke tab cakupan runtime instans EC2 dan filter menurut bidang nama Cluster untuk melihat Masalah terkait.

API/CLI

- Jalankan ListCoverageAPI dengan ID detektor valid Anda sendiri, Wilayah saat ini, dan titik akhir layanan. Anda dapat memfilter dan mengurutkan daftar instance menggunakan API ini.
  - Anda dapat mengubah contoh `filter-criteria` dengan salah satu opsi berikut untuk`CriterionKey`:
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`
  - Anda dapat mengubah contoh `AttributeName` `sort-criteria` dengan opsi berikut:
    - `ACCOUNT_ID`
    - `COVERAGE_STATUS`

    - ISSUE
    - ECS_CLUSTER_NAME
    - UPDATED_AT

      Bidang akan diperbarui hanya jika tugas baru dibuat di klaster Amazon ECS terkait atau ada perubahan dalam status cakupan yang sesuai.
  - Anda dapat mengubah *max-results* (hingga 50).
  - Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. detectorId

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Jalankan GetCoverageStatisticsAPI untuk mengambil statistik agregat cakupan berdasarkan. statisticsType
  - Anda dapat mengubah contoh statisticsType ke salah satu opsi berikut:
    - COUNT_BY_COVERAGE_STATUS— Merupakan statistik cakupan untuk cluster ECS yang dikumpulkan berdasarkan status cakupan.
    - COUNT_BY_RESOURCE_TYPE— Statistik cakupan dikumpulkan berdasarkan jenis AWS sumber daya dalam daftar.
    - Anda dapat mengubah contoh filter-criteria dalam perintah. Anda dapat menggunakan opsi berikut untukCriterionKey:
      - ACCOUNT_ID
      - ECS_CLUSTER_NAME
      - COVERAGE_STATUS
      - MANAGEMENT_TYPE
      - INSTANCE_ID
  - Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. detectorId

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
```

```
--filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
"FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Untuk informasi selengkapnya tentang masalah cakupan, lihatMemecahkan masalah cakupan ECS-Fargate runtime Amazon.

Perubahan status cakupan dengan EventBridge notifikasi

Status cakupan cluster Amazon ECS Anda mungkin tampak tidak sehat. Untuk mengetahui kapan status pertanggungan berubah, kami sarankan Anda untuk memantau status pertanggungan secara berkala, dan memecahkan masalah jika status menjadi tidak sehat. Atau, Anda dapat membuat EventBridge aturan Amazon untuk menerima pemberitahuan saat status cakupan berubah dari Tidak Sehat menjadi Sehat atau lainnya. Secara default, GuardDuty publikasikan ini di EventBridge bus untuk akun Anda.

Skema pemberitahuan sampel

Dalam EventBridge aturan, Anda dapat menggunakan contoh peristiwa dan pola peristiwa yang telah ditentukan sebelumnya untuk menerima pemberitahuan status cakupan. Untuk informasi selengkapnya tentang membuat EventBridge aturan, lihat Membuat aturan di Panduan EventBridge Pengguna Amazon.

Selain itu, Anda dapat membuat pola acara khusus dengan menggunakan skema pemberitahuan contoh berikut. Pastikan untuk mengganti nilai untuk akun Anda. Untuk mendapatkan pemberitahuan saat status cakupan klaster Amazon ECS Anda berubah dari `Healthy` ke`Unhealthy`, `detail-type` seharusnya begitu. *`GuardDuty Runtime Protection Unhealthy`* Untuk mendapatkan pemberitahuan ketika status cakupan berubah dari `Unhealthy` ke`Healthy`, ganti nilai `detail-type` dengan*`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Akun AWS ID",
  "time": "event timestamp (string)",
  "region": "Wilayah AWS",
  "resources": [
       ],
  "detail": {
```

```
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "ECS",
        "ecsClusterDetails": {
          "clusterName":"",
          "fargateDetails":{
            "issues":[],
            "managementType":""
          },
          "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
          }
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Memecahkan masalah cakupan ECS-Fargate runtime Amazon

Jika status cakupan klaster Amazon ECS Anda tidak sehat, Anda dapat melihat alasannya di bawah kolom Masalah.

Tabel berikut menyediakan langkah-langkah pemecahan masalah yang disarankan untuk masalah Fargate (hanya Amazon ECS). Untuk informasi tentang masalah cakupan instans Amazon EC2, lihat Memecahkan masalah cakupan runtime Amazon EC2 instans Amazon EC2.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
Agen tidak melaporkan	Agen tidak melaporkan tugas di `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Validasi bahwa titik akhir VPC untuk tugas klaster Amazon ECS Anda telah dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat Memvalidasi konfigurasi titik akhir VPC.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
		Jika organisasi Anda memiliki kebijakan kontrol layanan (SCP), validasi bahwa batas izin tidak membatasi izin. `guardduty:SendSecurityTelemetry` Untuk informasi selengkapnya, lihat Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun.
	VPC_ISSUE ; for task in TaskDefinition - '*TASK_DEFINITION* '	Lihat detail masalah VPC di informasi tambahan.
Agen keluar	ExitCode: `EXIT_CODE` untuk tugas di `TaskDefinition` - '*TASK_DEFINITION* '	Lihat detail masalah di informasi tambahan.
	Alasan: *REASON* untuk tugas-tugas di `TaskDefinition` - '*TASK_DEFINITION* '	
	ExitCode: `EXIT_CODE` dengan alasan: '*EXIT_CODE* ' untuk tugas di `TaskDefinition` - ' *TASK_DEFINITION* '	

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	Agen keluar: Alasan:`CannotPullContainerError` : tarik manifes gambar telah dicoba lagi...	Dalam skenario GuardDuty ini, berpotensi tidak dapat menarik gambar wadah sespan. Tugas Anda akan terus berjalan tetapi tidak GuardDuty dapat mendeteksi potensi ancaman. Lakukan langkah pemecahan masalah berikut satu per satu untuk memeriksa apakah itu membantu menyelesaikan masalah cakupan: • Izin: Pastikan peran eksekusi tugas Anda memiliki izin ECR yang diperlukan. Persyaratan izin • Konektivitas jaringan: Verifikasi bahwa tugas Fargate Anda dapat mencapai ECR baik melalui akses internet publik atau titik akhir VPC yang dikonfigurasi dengan benar seperti yang dijelaskan dalam. Persyaratan konektivitas jaringan • Konfigurasi grup keamanan: Periksa apakah grup keamanan Anda mengizinkan akses keluar ke daftar awalan terkelola S3 pada port 443 seperti yang

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
		dijelaskan di. Konfigurasi grup keamanan • Jalankan AWSSupport-TroubleshootECSTaskFailedToStartrunbook di Wilayah klaster Anda untuk mengidentifikasi masalah tertentu. • Lihat log tugas untuk pesan kesalahan. Untuk informasi tentang cara melakukan nya, lihat Melihat log agen kontainer Amazon ECS di Panduan Pengembang Layanan Kontainer Elastis Amazon. Untuk kesalahan umum dan pemecahan masalah, lihat Pemecahan masalah Amazon ECS di Panduan Pengembang Layanan Amazon Elastic Container. Ketiga komponen ini (izin, konektivitas jaringan, dan konfigurasi grup keamanan) bersifat independen tetapi semuanya diperlukan untuk berhasil mengunduh gambar GuardDuty kontainer dari Amazon ECR.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
		Jika masalah berlanjut, lihatSaya AWS Step Functions alur kerja gagal secara tak terduga.
Pembuatan Titik Akhir VPC Gagal	Mengaktifkan DNS pribadi memerlukan atribut keduanya dan `enableDnsSupport` `enableDnsHostnames` VPC disetel ke `true` for *`vpcId`* (Layanan: EC2, Status Code:400, ID Permintaan:). *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*	Pastikan atribut VPC berikut disetel ke `true` — `enableDnsSupport` dan. `enableDnsHostnames` Untuk informasi selengkapnya, lihat atribut DNS di VPC Anda. Jika Anda menggunakan Konsol VPC Amazon di https://console.aws.amazon.com/vpc/untuk membuat VPC Amazon, pastikan untuk memilih Aktifkan nama host DNS dan Aktifkan resolusi DNS. Untuk informasi selengkapnya, lihat opsi konfigurasi VPC.
	Pemanggilan yang tidak didukung oleh *`SERVICE`* untuk tugas di `TaskDefinition` `-` *`'TASK_DEFINITION '`*	Tugas ini dipanggil oleh a *`SERVICE`* yang tidak didukung.
Agen tidak disediakan	Arsitektur CPU yang tidak didukung *`TYPE`* " untuk tugas di `TaskDefinition` `-` *`'TASK_DEFINITION '`*	Tugas ini berjalan pada arsitektur CPU yang tidak didukung. Untuk informasi tentang arsitektur CPU yang didukung, lihatMemvalidasi persyaratan arsitektur.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	`TaskExecutionRole` hilang dari `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Peran eksekusi tugas ECS tidak ada. Untuk informasi tentang menyediakan peran eksekusi tugas dan izin yang diperlukan, lihatPrasyarat untuk akses gambar kontainer.
	Konfigurasi jaringan '*`CONFIGURATION_DETAILS`* ' tidak ada untuk tugas di `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Masalah konfigurasi jaringan mungkin muncul karena konfigurasi VPC yang hilang, atau subnet yang hilang atau kosong. Validasi bahwa konfigurasi jaringan Anda benar. Untuk informasi selengkapnya, lihat Prasyarat untuk akses gambar kontainer. Untuk informasi selengkapnya, lihat parameter definisi tugas Amazon ECS di Panduan Pengembang Layanan Kontainer Elastis Amazon.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	Tugas dimulai ketika cluster memiliki tag pengecualian dikecualikan dari Runtime Monitoring. ID tugas yang terkena dampak: '*TASK_ID*	Bila Anda mengubah GuardDuty tag yang telah ditentukan dari `GuardDuty Managed - true` ke `GuardDutyManaged -false`, tidak GuardDuty akan menerima peristiwa runtime untuk cluster Amazon ECS ini. Perbarui tag ke `GuardDuty Managed - true` dan kemudian luncurkan kembali tugas.
	Layanan yang diterapka n saat klaster memiliki tag pengecualian dikecualikan dari Runtime Monitoring. Nama layanan yang terkena dampak: " *SERVICE_NAME*	Ketika layanan diterapka n dengan tag pengecual ian `GuardDutyManaged -false`, tidak GuardDuty akan menerima peristiwa runtime untuk klaster Amazon ECS ini. Perbarui tag ke `GuardDuty Managed - true` dan kemudian gunakan kembali layanan.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	Tugas yang dimulai sebelum mengaktifkan Konfigurasi Agen Otomatis tidak tercakup. ID tugas yang terkena dampak: " *TASK_ID*	Ketika cluster berisi tugas yang diluncurkan sebelum mengaktifkan konfigurasi agen Otomatis untuk Amazon ECS, maka tidak GuardDuty akan dapat melindung i ini. Luncurkan kembali tugas untuk dipantau oleh. GuardDuty
	Layanan yang digunakan sebelum mengaktifkan Konfigurasi Agen Otomatis tidak tercakup. Nama layanan yang terkena dampak: " *SERVICE_NAME*	Ketika layanan diterapka n sebelum mengaktifkan konfigurasi agen Otomatis untuk Amazon ECS, tidak GuardDuty akan menerima peristiwa runtime untuk kluster ECS.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	Layanan '*SERVICE_NAME* ' membutuhkan penerapan baru ke fix/troubleshoot. Referensi kan dokumentasi, Nama layanan yang terkena dampak: " *SERVICE_NAME*	Layanan yang dimulai sebelum mengaktifkan Runtime Monitoring tidak didukung. Anda dapat memulai ulang layanan atau memperbarui layanan dengan `forceNewDeployment` opsi dengan mengikuti langkah-langkah di bawah Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container. Atau, Anda juga dapat menggunakan langkah-langkah UpdateServicedi bawah Referensi API Amazon Elastic Container Service.
	Tugas yang dimulai sebelum mengaktifkan Runtime Monitoring memerlukan peluncuran ulang. ID tugas yang terkena dampak: " *TASK_ID_1*	Di Amazon ECS, tugasnya tidak dapat diubah. Untuk menilai perilaku runtime atau AWS Fargate tugas yang sedang berjalan, pastikan Runtime Monitoring sudah diaktifkan, lalu restart tugas GuardDuty untuk menambahk an sespan container.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
Lainnya	Masalah tak dikenal, untuk tugas di `TaskDefinition - 'TASK_DEFINITION '`	Gunakan pertanyaan-pertanyaan berikut untuk mengidentifikasi akar penyebab masalah: • Apakah tugas dimulai sebelum Anda mengaktifkan Runtime Monitoring? Di Amazon ECS, tugasnya tidak dapat diubah. Untuk menilai perilaku runtime dari tugas Fargate yang sedang berjalan, pastikan Runtime Monitoring sudah diaktifkan, lalu restart tugas GuardDuty untuk menambahkan sespan container. • Apakah tugas ini bagian dari penerapan layanan yang dimulai sebelum Anda mengaktifkan Runtime Monitoring? Jika ya, Anda dapat memulai ulang layanan atau memperbarui layanan `forceNewDeployment` dengan menggunakan langkah-langkah dalam Memperbarui layanan. Anda juga dapat menggunakan UpdateService atau AWS CLI.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
		• Apakah tugas diluncurkan setelah mengecualikan cluster ECS dari Runtime Monitoring? Saat Anda mengubah GuardDuty tag yang telah ditentukan sebelumnya dari `GuardDutyManaged - true` ke `GuardDuty Managed -false`, tidak GuardDuty akan menerima peristiwa runtime untuk cluster ECS. • Apakah layanan Anda berisi tugas yang memiliki format lama`taskArn`? GuardDuty Runtime Monitoring tidak mendukung cakupan untuk tugas yang memiliki format lama. `taskArn` Untuk informasi tentang Nama Sumber Daya Amazon (ARN) untuk sumber daya Amazon ECS, lihat Nama Sumber Daya Amazon (ARN) dan ID.

Cakupan runtime dan pemecahan masalah untuk klaster Amazon EKS

Setelah Anda mengaktifkan Runtime Monitoring dan menginstal agen GuardDuty keamanan (add-on) untuk EKS baik secara manual atau melalui konfigurasi agen otomatis, Anda dapat mulai menilai cakupan untuk kluster EKS Anda.

Daftar Isi

- Meninjau statistik cakupan
- Perubahan status cakupan dengan EventBridge notifikasi
- Memecahkan masalah cakupan runtime Amazon EKS

Meninjau statistik cakupan

Statistik cakupan untuk kluster EKS yang terkait dengan akun Anda sendiri atau akun anggota Anda adalah persentase kluster EKS yang sehat di semua kluster EKS yang dipilih. Wilayah AWS Persamaan berikut mewakili ini sebagai:

(clusters/All Cluster sehat) * 100

Pilih salah satu metode akses untuk meninjau statistik cakupan akun Anda.

Console

- Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
- Di panel navigasi, pilih Runtime Monitoring.
- Pilih tab cakupan runtime cluster EKS.
- Di bawah tab cakupan runtime kluster EKS, Anda dapat melihat statistik cakupan yang dikumpulkan berdasarkan status cakupan yang tersedia di tabel daftar Clusters.
  - Anda dapat memfilter tabel daftar Clusters dengan kolom berikut:
    - Nama cluster
    - ID Akun
    - Jenis manajemen agen
    - Status cakupan
    - Add-on versi

- Jika salah satu kluster EKS Anda memiliki status Cakupan sebagai Tidak Sehat, kolom Masalah dapat menyertakan informasi tambahan tentang alasan status Tidak Sehat.

API/CLI

- Jalankan ListCoverageAPI dengan ID detektor, Wilayah, dan titik akhir layanan Anda yang valid. Anda dapat memfilter dan mengurutkan daftar cluster menggunakan API ini.
  - Anda dapat mengubah contoh `filter-criteria` dengan salah satu opsi berikut untuk`CriterionKey`:
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `ADDON_VERSION`
    - `MANAGEMENT_TYPE`
  - Anda dapat mengubah contoh `AttributeName` `sort-criteria` dengan opsi berikut:
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `ISSUE`
    - `ADDON_VERSION`
    - `UPDATED_AT`
  - Anda dapat mengubah *`max-results`* (hingga 50).
  - Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Jalankan GetCoverageStatisticsAPI untuk mengambil statistik agregat cakupan berdasarkan. `statisticsType`

- Anda dapat mengubah contoh `statisticsType` ke salah satu opsi berikut:
  - `COUNT_BY_COVERAGE_STATUS`— Merupakan statistik cakupan untuk kluster EKS yang dikumpulkan berdasarkan status cakupan.
  - `COUNT_BY_RESOURCE_TYPE`— Statistik cakupan dikumpulkan berdasarkan jenis AWS sumber daya dalam daftar.
  - Anda dapat mengubah contoh `filter-criteria` dalam perintah. Anda dapat menggunakan opsi berikut untuk`CriterionKey`:
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `ADDON_VERSION`
    - `MANAGEMENT_TYPE`
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Jika status cakupan cluster EKS Anda tidak sehat, lihatMemecahkan masalah cakupan runtime Amazon EKS.

Perubahan status cakupan dengan EventBridge notifikasi

Status cakupan klaster EKS di akun Anda mungkin muncul sebagai Tidak Sehat. Untuk mendeteksi kapan status pertanggungan menjadi tidak sehat, kami sarankan Anda memantau status pertanggungan secara berkala dan memecahkan masalah, jika statusnya tidak sehat. Atau, Anda dapat membuat EventBridge aturan Amazon untuk memberi tahu Anda ketika status cakupan berubah dari salah satu `Unhealthy` ke `Healthy` atau sebaliknya. Secara default, GuardDuty publikasikan ini di EventBridge bus untuk akun Anda.

Skema pemberitahuan sampel

Dalam EventBridge aturan, Anda dapat menggunakan contoh peristiwa dan pola peristiwa yang telah ditentukan sebelumnya untuk menerima pemberitahuan status cakupan. Untuk informasi selengkapnya tentang membuat EventBridge aturan, lihat Membuat aturan di Panduan EventBridge Pengguna Amazon.

Selain itu, Anda dapat membuat pola acara khusus dengan menggunakan skema pemberitahuan contoh berikut. Pastikan untuk mengganti nilai untuk akun Anda. Untuk mendapatkan pemberitahuan saat status cakupan klaster Amazon EKS Anda berubah dari `Healthy` ke`Unhealthy`, `detail-type` seharusnya *`GuardDuty Runtime Protection Unhealthy`* begitu. Untuk mendapatkan pemberitahuan ketika status cakupan berubah dari `Unhealthy` ke`Healthy`, ganti nilai `detail-type` dengan*`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Akun AWS ID",
  "time": "event timestamp (string)",
  "region": "Wilayah AWS",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EKS",
        "eksClusterDetails": {
            "clusterName": "string",
            "availableNodes": "string",
             "desiredNodes": "string",
             "addonVersion": "string"
         }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Memecahkan masalah cakupan runtime Amazon EKS

Jika status cakupan untuk kluster EKS AndaUnhealthy, Anda dapat melihat kesalahan terkait baik di bawah kolom Masalah di GuardDuty konsol, atau dengan menggunakan tipe CoverageResourcedata.

Saat bekerja dengan tag inklusi atau pengecualian untuk memantau kluster EKS Anda secara selektif, mungkin perlu beberapa waktu bagi tag untuk disinkronkan. Ini dapat memengaruhi status cakupan cluster EKS terkait. Anda dapat mencoba menghapus dan menambahkan tag yang sesuai (penyertaan atau pengecualian) lagi. Untuk informasi selengkapnya, lihat Menandai sumber daya Amazon EKS Anda di Panduan Pengguna Amazon EKS.

Struktur masalah cakupan adalahIssue type:Extra information. Biasanya, masalah akan memiliki informasi Tambahan opsional yang mungkin mencakup pengecualian atau deskripsi sisi klien tertentu tentang masalah tersebut. Berdasarkan informasi tambahan, tabel berikut memberikan langkah-langkah yang disarankan untuk memecahkan masalah cakupan untuk kluster EKS Anda.

Jenis masalah (awalan)	Informasi tambahan	Langkah pemecahan masalah yang disarankan
Pembuatan Addon Gagal	Addon tidak aws-guard duty-agent kompatibe l dengan versi cluster cluster saat ini. *ClusterName* Addon ditentukan tidak didukung.	Pastikan Anda menggunakan salah satu versi Kubernetes yang mendukung penerapan add-on EKS. aws-guard duty-agent Untuk informasi selengkapnya, lihat Versi Kubernetes didukung oleh agen keamanan GuardDuty. Untuk informasi tentang memperbarui versi Kubernetes Anda, lihat Memperbarui versi Kubernetes klaster Amazon EKS.
Pembuatan Addon Gagal Pembaruan Addon Gagal Addon Status Tidak Sehat	Masalah EKS Addon -AddonIssueCode : AddonIssueMessage	Untuk informasi tentang langkah-langkah yang disarankan untuk kode masalah add-on tertentu,

Jenis masalah (awalan)	Informasi tambahan	Langkah pemecahan masalah yang disarankan
		lihatTroubleshooting steps for Addon creation/update error with Addon issue code. Untuk daftar kode masalah addon yang mungkin Anda alami dalam masalah ini, lihat AddonIssue.
Pembuatan Titik Akhir VPC Gagal	Pembuatan titik akhir VPC tidak didukung untuk VPC bersama *vpcId*	Runtime Monitoring sekarang mendukung penggunaan VPC bersama dalam suatu organisasi. Pastikan akun Anda memenuhi semua prasyarat. Untuk informasi selengkapnya, lihat Prasyarat untuk menggunakan VPC bersama.
	Hanya saat menggunakan VPC bersama dengan konfigurasi agen otomatis ID akun pemilik *111122223333* untuk VPC bersama *vpcId* tidak mengaktifkan Runtime Monitoring, konfigurasi agen otomatis, atau keduanya.	Akun pemilik VPC bersama harus mengaktifkan Runtime Monitoring dan konfigurasi agen otomatis untuk setidaknya satu jenis sumber daya (Amazon EKS atau Amazon ECS ()).AWS Fargate Untuk informasi selengkapnya, lihat Prasyarat khusus untuk Runtime Monitoring GuardDuty.

Jenis masalah (awalan)	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	Mengaktifkan DNS pribadi memerlukan atribut keduanya dan `enableDnsSupport` `enableDnsHostnames` VPC disetel ke `true` for *`vpcId`* (Layanan: Ec2, Status Code:400, ID Permintaan:). *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*	Pastikan atribut VPC berikut disetel ke `true` — `enableDnsSupport` dan. `enableDnsHostnames` Untuk informasi selengkapnya, lihat atribut DNS di VPC Anda. Jika Anda menggunakan Konsol VPC Amazon di https://console.aws.amazon.com/vpc/untuk membuat VPC Amazon, pastikan untuk memilih Aktifkan nama host DNS dan Aktifkan resolusi DNS. Untuk informasi selengkapnya, lihat opsi konfigurasi VPC.

Jenis masalah (awalan)	Informasi tambahan	Langkah pemecahan masalah yang disarankan
Penghapusan Titik Akhir VPC Bersama Gagal	Penghapusan titik akhir VPC bersama tidak diizinkan untuk ID akun, VPC *111122223333* bersama, ID akun pemilik. *vpcId 555555555555*	Langkah-langkah potensial: • Menonaktifkan status Pemantauan Waktu Proses akun peserta VPC bersama tidak memengaruhi kebijakan titik akhir VPC bersama dan grup keamanan yang ada di akun pemilik. Untuk menghapus titik akhir VPC bersama dan grup keamanan, Anda harus menonaktifkan Pemantauan Waktu Proses atau status konfigurasi agen otomatis di akun pemilik VPC bersama. • Akun peserta VPC bersama tidak dapat menghapus titik akhir VPC bersama dan grup keamanan yang dihosting di akun pemilik VPC bersama.
Cluster EKS lokal	Addon EKS tidak didukung pada kluster pos terdepan lokal.	Tidak bisa ditindaklanjuti. Untuk informasi lebih lanjut, lihat Amazon EKS di AWS pos terdepan.

Jenis masalah (awalan)	Informasi tambahan	Langkah pemecahan masalah yang disarankan
Izin pengaktifan Pemantauan Runtime EKS tidak diberikan	(mungkin atau mungkin tidak menampilkan informasi tambahan)	1. Jika informasi tambahan tersedia untuk masalah ini, perbaiki akar penyebabnya dan ikuti langkah berikutnya. 2. Alihkan EKS Runtime Monitoring untuk mematikannya dan kemudian menyalakannya kembali. Pastikan bahwa GuardDuty agen juga dikerahkan, baik secara otomatis melalui GuardDuty atau manual.
EKS Runtime Monitoring pemberdayaan penyediaan sumber daya sedang berlangsung	(mungkin atau mungkin tidak menampilkan informasi tambahan)	Tidak bisa ditindaklanjuti. Setelah Anda mengaktifkan EKS Runtime Monitoring, status cakupan mungkin tetap ada `Unhealthy` hingga langkah penyediaan sumber daya selesai. Status cakupan dipantau dan diperbarui secara berkala.
Lainnya (masalah lainnya)	Kesalahan karena kegagalan otorisasi	Alihkan EKS Runtime Monitoring untuk mematikannya dan kemudian menyalakannya kembali. Pastikan GuardDuty agen juga dikerahkan, baik secara otomatis melalui GuardDuty atau manual.

Langkah-langkah pemecahan masalah untuk creation/update kesalahan Addon dengan kode masalah Addon

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
EKS Addon Issue -`InsufficientNumberOfReplicas` : Add-on tidak sehat karena tidak memiliki jumlah replika yang diinginkan.	• Dengan menggunakan pesan masalah, Anda dapat mengidentifikasi dan memperbaiki akar masalahnya. Anda bisa mulai dengan mendeskripsikan cluster Anda. Misalnya, gunakan `kubectl describe pods`untuk mengidentifikasi akar penyebab kegagalan pod. Setelah Anda memperbaiki akar penyebabn ya, coba lagi langkahnya (pembuatan atau pembaruan add-on). • Jika masalah berlanjut, validasi bahwa titik akhir VPC untuk kluster Amazon EKS Anda telah dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat Memvalidasi konfigurasi titik akhir VPC.
EKS Addon Issue -`InsufficientNumberOfReplicas` : Add-on tidak sehat karena satu atau lebih pod tidak dijadwalkan `0/x` node tersedia:. `x Insufficient cpu. preemption: not eligible due to preemptionPolicy=Never`	Untuk mengatasi masalah ini, Anda dapat melakukan salah satu dari yang berikut: • Perbarui prioritas pod GuardDuty agen: Parameter dan nilai yang dapat dikonfigu rasi dengan menyetel `PriorityC lass` ke salah satu opsi yang mendukung `preemptionPolicy` nilai sebagai`PreemptLowerPriority` . Untuk informasi tentang prioritas pod, lihat Prioritas Pod dan Preemption di Dokumenta si Kubernetes. • Tingkatkan instans: Untuk mengelola sumber daya dan membuat pemilihan instans
EKS Addon Issue -`InsufficientNumberOfReplicas` : Add-on tidak sehat karena satu atau lebih pod tidak dijadwalkan `0/x` node tersedia:. `x Too many pods. preemptio n: not eligible due to preemptio nPolicy=Never`	

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
EKS Addon Issue -`InsufficientNumberOfReplicas` : Add-on tidak sehat karena satu atau lebih pod tidak dijadwalkan `0/x` node tersedia:. `1 Insufficient memory. preemption: not eligible due to preemptionPolicy=Never`	yang optimal, lihat Mengelola sumber daya komputasi menggunakan node dan Pilih jenis instans node Amazon EC2 yang optimal di Panduan Pengguna Amazon EKS. **Note** Pesan ditampilkan `0/x` karena hanya GuardDuty melaporkan kesalahan pertama yang ditemukan. Jumlah sebenarnya dari pod yang berjalan di GuardDuty daemonset mungkin lebih besar dari 0.

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
Masalah EKS Addon -`InsufficientNumberOfReplicas` : Add-on tidak sehat karena satu atau lebih pod memiliki wadah yang menunggu `CrashLoopBackOff: Completed`	Anda dapat melihat log yang terkait dengan pod dan mengidentifikasi masalahnya. Untuk informasi tentang cara melakukannya, lihat Debug Running Pods di Dokumentasi Kubernetes. Gunakan daftar periksa berikut untuk memecahkan masalah add-on ini: • Validasi bahwa Runtime Monitoring diaktifkan. • Validasi bahwaPrasyarat untuk dukungan klaster Amazon EKS, seperti distribusi OS terverifikasi dan versi Kubernetes yang didukung, terpenuhi. • Saat Anda mengelola agen keamanan secara manual, konfirmasikan bahwa Anda membuat titik akhir VPC untuk semua VPC. Saat Anda mengaktifkan konfigurasi GuardDuty otomatis, Anda tetap harus memvalidasi bahwa titik akhir VPC dibuat. Misalnya, saat menggunakan VPC bersama dalam konfigurasi otomatis. Untuk memvalidasi ini, lihatMemvalidasi konfigurasi titik akhir VPC. • Konfirmasikan bahwa agen GuardDuty keamanan dapat menyelesaikan DNS GuardDuty pribadi titik akhir VPC. Untuk mengetahui titik akhir, lihat Nama DNS pribadi untuk titik akhir di. Mengelola agen GuardDuty keamanan

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
	Untuk melakukan ini, Anda dapat menggunakan `nslookup` alat di Windows atau Mac, atau `dig` alat di Linux. Saat menggunakan nslookup, Anda dapat menggunakan perintah berikut setelah mengganti Region *`us-west-2`* dengan Region Anda: `nslookup guardduty-data.` *`us-west-2`* `.amazonaws.com` • Validasi bahwa kebijakan titik akhir GuardDuty VPC Anda atau kebijakan kontrol layanan tidak memengaruhi tindakan. `guardduty:SendSecurityTelemetry`

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
Masalah EKS Addon -`InsufficientNumberOfReplicas` : Add-on tidak sehat karena satu atau lebih pod memiliki wadah yang menunggu `CrashLoopBackOff: Error`	Anda dapat melihat log yang terkait dengan pod dan mengidentifikasi masalahnya. Untuk informasi tentang cara melakukannya, lihat Debug Running Pods di Dokumentasi Kubernetes. Setelah Anda mengidentifikasi masalah, gunakan daftar periksa berikut untuk memecahkan masalah ini: • Validasi bahwa Runtime Monitoring diaktifkan. • Validasi bahwaPrasyarat untuk dukungan klaster Amazon EKS, seperti distribusi OS terverifikasi dan versi Kubernetes yang didukung, terpenuhi. • Agen GuardDuty keamanan dapat menyelesaikan DNS pribadi titik akhir GuardDuty VPC. Untuk mengetahui titik akhir, lihat Nama DNS pribadi untuk titik akhir di. Mengelola agen GuardDuty keamanan
Masalah EKS Addon -`AdmissionRequestDenied` : webhook penerimaan `"validate.kyverno.svc-fail"` menolak permintaan: kebijakan `DaemonSet/amazon-guardduty/aws-guardduty-agent` untuk pelanggaran sumber daya: restrict-image-registries::... `autogen-validate-registries`	1. Cluster Amazon EKS atau administrator keamanan harus meninjau kebijakan keamanan yang memblokir pembaruan Addon. 2. Anda harus menonaktifkan controller (`webhook`) atau meminta controller menerima permintaan dari Amazon EKS.

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
EKS Addon Issue -`ConfigurationConflict` : Konflik ditemukan saat mencoba menerapkan. Tidak akan berlanjut karena menyelesaikan mode konflik. `Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image`	Saat membuat atau memperbarui Addon, berikan bendera `OVERWRITE` konflik penyelesaian. Ini berpotensi menimpa setiap perubahan yang telah dibuat langsung ke sumber daya terkait di Kubernetes dengan menggunakan API Kubernetes. Anda dapat terlebih dahulu Menghapus add-on Amazon EKS dari cluster dan kemudian menginstal ulang.

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah

Masalah EKS Addon - `AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope`	Anda harus menambahkan izin yang hilang ke `eks:addon-cluster-admin ClusterRoleBinding` manual. Tambahkan yang berikut ini `yaml` ke`eks:addon-cluster-admin` :
	`---`
	`kind: ClusterRoleBinding`
	`apiVersion: rbac.authorization.k8s.io/v1`
	`metadata:`
	`  name: eks:addon-cluster-admin`
	`subjects:`
	`- kind: User`
	`  name: eks:addon-manager`
	`  apiGroup: rbac.authorization.k8s.io`
	`roleRef:`
	`  kind: ClusterRole`
	`  name: cluster-admin`
	`  apiGroup: rbac.authorization.k8s.io`
	`---`
	Anda sekarang dapat menerapkan ini `yaml` ke cluster Amazon EKS Anda dengan menggunakan perintah berikut:
	`kubectl apply -f eks-addon-cluster-admin.yaml`

AddonUpdationFailed: EKSAddonIssue - `AccessDenied: namespaces\"amazon-guardduty\"isforbidden:User\"eks:addon-manager\"cannotpatchresource\"namespaces\"inAPIgroup\"\"inthenamespace\"amazon-guardduty\"`	

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
Masalah EKS Addon - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label`	Anda harus menonaktifkan pengontrol atau meminta pengontrol menerima permintaan dari kluster Amazon EKS. Sebelum membuat atau memperbarui add-on, Anda juga dapat membuat GuardDuty namespace dan memberi label sebagai. `owner`
Masalah EKS Addon - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [allowed-container-registries] container <aws-guardduty-agent> has an invalid image registry`	Tambahkan registri gambar GuardDuty ke `allowed-container-registries` dalam pengontrol penerimaan Anda. Untuk informasi lebih lanjut, lihat repositori ECR untuk EKS v1.8.1-eks-build.2 di. Agen hosting repositori Amazon ECR GuardDuty

Menyiapkan CPU dan pemantauan memori

Setelah mengaktifkan Runtime Monitoring dan menilai bahwa status cakupan klaster Anda Sehat, Anda dapat menyiapkan dan melihat metrik wawasan.

Topik berikut dapat membantu Anda mengevaluasi kinerja agen yang digunakan terhadap CPU dan batas memori untuk GuardDuty agen.

Menyiapkan pemantauan di Amazon ECS cluster

Langkah-langkah berikut dari Panduan CloudWatch Pengguna Amazon dapat membantu Anda mengevaluasi kinerja agen yang digunakan terhadap batas CPU dan memori GuardDuty agen:

1. Menyiapkan Wawasan Kontainer di Amazon ECS untuk metrik tingkat kluster dan layanan
2. Metrik Wawasan Kontainer Amazon ECS

Menyiapkan pemantauan di klaster Amazon EKS

Setelah agen GuardDuty keamanan diterapkan dan Anda menilai bahwa status cakupan klaster Anda Sehat, Anda dapat mengatur dan melihat metrik Wawasan Kontainer.

Mengevaluasi kinerja agen keamanan

1. Menyiapkan Wawasan Kontainer di Amazon EKS dan Kubernetes di Panduan Pengguna Amazon CloudWatch
2. Metrik Amazon EKS dan Kubernetes Container Insights di Panduan Pengguna Amazon CloudWatch

Mengelola kinerja dengan agen keamanan v1.5.0 ke atas

Dengan agen keamanan v1.5.0 dan yang lebih baru, ketika wawasan menunjukkan bahwa GuardDuty agen terkait mencapai batas yang ditetapkan, Anda dapat mengonfigurasi parameter tertentu. Untuk informasi selengkapnya, lihat Konfigurasikan parameter add-on EKS.

Menggunakan VPC bersama dengan Runtime Monitoring

GuardDuty Runtime Monitoring mendukung penggunaan Amazon Virtual Private Cloud bersama (Amazon VPC) untuk Akun AWS Anda yang termasuk dalam organisasi yang sama di. AWS Organizations Anda dapat menggunakan VPC bersama dengan dua cara:

- Konfigurasi agen otomatis (Disarankan) — Saat mengelola agen keamanan GuardDuty secara otomatis, itu juga akan mengonfigurasi kebijakan titik akhir VPC Amazon. Kebijakan ini didasarkan pada setelan VPC bersama organisasi Anda.

  Anda harus mengaktifkan konfigurasi agen otomatis di akun pemilik VPC bersama dan semua akun yang berpartisipasi yang akan membagikan VPC ini.
- Agen yang dikelola secara manual — Saat Anda mengelola agen keamanan secara manual dengan VPC bersama, Anda harus memperbarui kebijakan titik akhir VPC untuk mengizinkan akun terkait mengakses VPC bersama. Untuk melakukannya, Anda dapat menggunakan kebijakan contoh yang dibagikan di Cara kerjanya bagian berikut.

  Untuk skenario manajemen manual yang melibatkan akun yang berpartisipasi untuk VPC bersama, status pertanggungan mungkin tidak akurat. Untuk memastikan perlindungan terkini dan status cakupan sumber daya Anda, GuardDuty rekomendasikan untuk mengaktifkan konfigurasi agen otomatis untuk semua akun yang akan menggunakan VPC bersama.

Topik

- Cara kerjanya
- Prasyarat untuk menggunakan VPC bersama

Cara kerjanya

Yang Akun AWS termasuk dalam organisasi yang sama dengan akun pemilik VPC Amazon bersama juga dapat berbagi titik akhir VPC Amazon yang sama. Setiap akun yang berbagi VPC Amazon yang sama disebut AWS akun peserta dari VPC Amazon bersama yang terkait.

Contoh berikut menunjukkan kebijakan titik akhir VPC default dari akun pemilik VPC bersama dan akun peserta. Ini `aws:PrincipalOrgID` akan menampilkan ID organisasi yang terkait dengan sumber daya VPC bersama. Penggunaan kebijakan ini terbatas pada akun peserta yang ada dalam organisasi akun pemilik.

Example Contoh kebijakan titik akhir VPC bersama

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
        }
    ]
}
```

Dengan konfigurasi agen GuardDuty otomatis

Saat akun pemilik VPC bersama mengaktifkan Pemantauan Waktu Proses dan konfigurasi agen otomatis untuk sumber daya apa pun (Amazon EKS atau (hanya AWS Fargate Amazon ECS)), semua VPC bersama memenuhi syarat untuk penginstalan otomatis titik akhir VPC Amazon bersama dan grup keamanan terkait di akun pemilik VPC bersama. GuardDuty mengambil ID organisasi yang terkait dengan VPC Amazon bersama.

GuardDuty membuat titik akhir VPC Amazon saat akun pemilik VPC bersama atau akun yang berpartisipasi membutuhkannya. Contoh membutuhkan endpoint VPC Amazon termasuk GuardDuty mengaktifkan, Runtime Monitoring, EKS Runtime Monitoring, atau meluncurkan tugas Amazon baru. ECS-Fargate Jika akun ini mengaktifkan Pemantauan Waktu Proses dan konfigurasi agen otomatis untuk semua jenis sumber daya, GuardDuty buat titik akhir VPC Amazon dan tetapkan kebijakan titik akhir dengan ID organisasi yang sama dengan akun pemilik VPC bersama. GuardDuty menambahkan `GuardDutyManaged` tag dan menyetelnya `true` untuk titik akhir VPC Amazon yang dibuat. GuardDuty Jika akun pemilik VPC Amazon bersama belum mengaktifkan Pemantauan Waktu Proses atau konfigurasi agen otomatis untuk salah satu sumber daya, tidak GuardDuty akan menetapkan kebijakan titik akhir VPC Amazon. Untuk informasi tentang mengonfigurasi Runtime Monitoring dan mengelola agen keamanan secara otomatis di akun pemilik VPC bersama, lihat. Mengaktifkan GuardDuty Runtime Monitoring

Menggunakan dengan agen yang dikelola secara manual

Saat Anda menggunakan VPC bersama dengan agen yang dikelola secara manual, validasi bahwa tidak ada kebijakan `Deny` titik akhir eksplisit yang memblokir akun apa pun yang perlu menggunakan VPC bersama. Ini mencegah agen keamanan mengirim telemetri ke GuardDuty, menghasilkan status `Unhealthy` cakupan. Untuk menyiapkan kebijakan titik akhir, lihatExample shared VPC endpoint policy.

Cakupan runtime mungkin tidak akurat dalam skenario seperti izin yang hilang ke VPC bersama. Anda dapat terus memantau cakupan sumber daya dengan mengikuti langkah-langkah untuk jenis sumber daya AndaMeninjau statistik cakupan runtime dan masalah pemecahan masalah.

Untuk memastikan perlindungan Runtime Monitoring berkelanjutan dari sumber daya komputasi Anda, GuardDuty rekomendasikan untuk mengaktifkan konfigurasi agen otomatis untuk akun pemilik VPC bersama dan semua akun yang berpartisipasi untuk sumber daya Anda.

Prasyarat untuk menggunakan VPC bersama

Sebagai bagian dari pengaturan awal, lakukan langkah-langkah berikut di Akun AWS mana Anda ingin menjadi pemilik VPC bersama:

1. Membuat organisasi — Membuat organisasi dengan mengikuti langkah-langkah dalam Membuat dan mengelola organisasi dalam Panduan AWS Organizations Pengguna.

   Untuk informasi tentang menambahkan atau menghapus akun anggota, lihat Mengelola Akun AWS di organisasi Anda.
2. Membuat sumber daya VPC bersama — Anda dapat membuat sumber daya VPC bersama dari akun pemilik. Untuk informasi selengkapnya, lihat Berbagi subnet VPC Anda dengan akun lain di Panduan Pengguna Amazon VPC.

Prasyarat khusus untuk Runtime Monitoring GuardDuty

Daftar berikut memberikan prasyarat yang khusus untuk: GuardDuty

- Akun pemilik VPC bersama dan akun yang berpartisipasi dapat berasal dari berbagai organisasi di. GuardDuty Namun, mereka harus menjadi anggota organisasi yang sama di AWS Organizations. Ini diperlukan GuardDuty untuk membuat titik akhir VPC Amazon dan grup keamanan untuk VPC bersama. Untuk informasi tentang cara kerja VPC bersama, lihat Membagikan VPC Anda dengan akun lain di Panduan Pengguna Amazon VPC.
- Aktifkan Runtime Monitoring atau EKS Runtime Monitoring, dan konfigurasi agen GuardDuty otomatis untuk sumber daya apa pun di akun pemilik VPC bersama dan akun peserta. Untuk informasi selengkapnya, lihat Mengaktifkan Runtime Monitoring.

  Jika Anda telah menyelesaikan konfigurasi ini, lanjutkan dengan langkah berikutnya.
- Saat bekerja dengan Amazon EKS atau tugas Amazon ECS (AWS Fargate hanya), pastikan untuk memilih sumber daya VPC bersama yang terkait dengan akun pemilik dan pilih subnetnya.

Menggunakan Infrastructure as Code (IAc) dengan GuardDuty agen keamanan otomatis

Gunakan bagian ini hanya jika daftar berikut berlaku untuk kasus penggunaan Anda:

- Anda menggunakan alat Infrastructure as Code (IAc), seperti AWS Cloud Development Kit (AWS CDK) dan Terraform, untuk mengelola sumber daya Anda AWS , dan
- Anda perlu mengaktifkan konfigurasi agen GuardDuty otomatis untuk satu atau beberapa jenis sumber daya - Amazon EKS, Amazon EC2, atau Amazon. ECS-Fargate

Ikhtisar grafik ketergantungan sumber daya IAc

Saat Anda mengaktifkan konfigurasi agen GuardDuty otomatis untuk jenis sumber daya, GuardDuty secara otomatis membuat titik akhir VPC dan grup keamanan yang terkait dengan titik akhir VPC ini, dan menginstal agen keamanan untuk jenis sumber daya ini. Secara default, GuardDuty akan menghapus titik akhir VPC dan grup keamanan terkait hanya setelah Anda menonaktifkan Runtime Monitoring. Untuk informasi selengkapnya, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Ketika Anda menggunakan alat IAc, ia mempertahankan grafik ketergantungan sumber daya. Pada saat penghapusan sumber daya menggunakan alat IAc, itu hanya menghapus sumber daya yang dapat dilacak sebagai bagian dari grafik ketergantungan sumber daya. Alat IAC mungkin tidak tahu tentang sumber daya yang dibuat di luar konfigurasi yang ditentukan. Misalnya, Anda membuat VPC dengan alat IAc dan kemudian menambahkan grup keamanan ke VPC ini dengan menggunakan AWS konsol atau operasi API. Dalam grafik ketergantungan sumber daya, sumber daya VPC yang Anda buat bergantung pada grup keamanan terkait. Jika Anda menghapus sumber daya VPC ini dengan menggunakan alat IAc, maka Anda akan mendapatkan kesalahan. Cara untuk mengatasi kesalahan ini adalah dengan menghapus grup keamanan terkait secara manual atau memperbarui konfigurasi IAC untuk memasukkan sumber daya tambahan ini.

Masalah umum - Menghapus sumber daya di IAc

Saat menggunakan konfigurasi agen GuardDuty otomatis, Anda mungkin ingin menghapus sumber daya (Amazon EKS, Amazon EC2, atau Amazon ECS-Fargate) yang Anda buat dengan menggunakan alat IAc. Namun, sumber daya ini bergantung pada titik akhir VPC yang dibuat. GuardDuty Ini mencegah alat IAC untuk menghapus sumber daya dengan sendirinya dan mengharuskan Anda untuk menonaktifkan Runtime Monitoring, yang selanjutnya menghapus titik akhir VPC secara otomatis.

Misalnya, ketika Anda mencoba menghapus titik akhir VPC yang GuardDuty dibuat atas nama Anda, Anda akan mendapatkan kesalahan yang mirip dengan contoh berikut.

Example

Contoh kesalahan saat menggunakan CDK

```
The following resource(s) failed to delete:
 [mycdkvpcapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpcapplicationprivatesubnet1Subne
Resource handler returned message: "The subnet 'subnet-APKAEIVFHP46CEXAMPLE' has
 dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request
 ID: e071c3c5-7442-4489-838c-0dfc6EXAMPLE)" (RequestToken: 4381cff8-6240-208a-8357-5557b7EXAMPL
 HandlerErrorCode: InvalidRequest)
```

Example

Contoh kesalahan saat menggunakan Terraform

```
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
 19m50s elapsed]
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
 20m0s elapsed]

Error: deleting EC2 Subnet (subnet-APKAEIBAERJR2EXAMPLE): DependencyViolation: The
 subnet 'subnet-APKAEIBAERJR2EXAMPLE' has dependencies and cannot be deleted.
       status code: 400, request id: e071c3c5-7442-4489-838c-0dfc6EXAMPLE
```

> **Note**
>
> AWS Penyedia Terraform versi 6.43.0 dan yang lebih baru menyelesaikan masalah ini secara otomatis. AWS Penyedia mendeteksi dan menghapus titik akhir GuardDuty-managed VPC dan grup keamanan selama. `terraform destroy` Perbaikan ini berlaku untuk semua jenis sumber daya (Amazon EKS, Amazon EC2, dan Amazon ECS-Fargate).

Solusi - Mencegah masalah penghapusan sumber daya

Bagian ini membantu Anda mengelola titik akhir VPC dan grup keamanan secara independen. GuardDuty

Untuk mendapatkan kepemilikan penuh atas sumber daya yang dikonfigurasi dengan menggunakan alat IAc, lakukan langkah-langkah berikut dalam urutan yang tercantum:

1. Buat sebuah VPC. Untuk mengizinkan izin masuk, kaitkan titik akhir GuardDuty VPC dengan grup keamanan, ke VPC ini.
2. Aktifkan konfigurasi agen GuardDuty otomatis untuk jenis sumber daya Anda

Setelah Anda menyelesaikan langkah-langkah sebelumnya, tidak GuardDuty akan membuat titik akhir VPC sendiri dan akan menggunakan kembali salah satu yang Anda buat dengan menggunakan alat IAc.

Untuk informasi tentang membuat VPC Anda sendiri, lihat Membuat VPC hanya di Gateway Transit VPC Amazon. Untuk informasi tentang membuat titik akhir VPC, lihat bagian berikut untuk jenis sumber daya Anda:

- Untuk Amazon EC2, lihat. Prasyarat - Membuat titik akhir Amazon VPC secara manual
- Untuk Amazon EKS, lihatPrasyarat - Membuat titik akhir VPC Amazon.

Jenis acara runtime yang dikumpulkan yang menggunakan GuardDuty

Agen GuardDuty keamanan mengumpulkan jenis peristiwa berikut dan mengirimkannya ke GuardDuty backend untuk deteksi dan analisis ancaman. GuardDuty tidak membuat acara ini dapat diakses oleh Anda. Jika GuardDuty mendeteksi potensi ancaman dan menghasilkanJenis penemuan Runtime Monitoring, Anda dapat melihat detail temuan yang sesuai.

Untuk informasi tentang cara GuardDuty menggunakan jenis peristiwa yang dikumpulkan di Runtime Monitoring, lihatMemilih untuk tidak menggunakan data Anda untuk perbaikan layanan.

Memproses acara

Peristiwa proses mewakili informasi yang terkait dengan proses yang berjalan di instans Amazon EC2 dan beban kerja kontainer. Tabel berikut mencakup nama bidang dan deskripsi peristiwa proses yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Nama proses	Nama proses yang diamati.

Nama bidang	Deskripsi
Jalur Proses	Jalur absolut dari proses yang dapat dieksekusi.
ID Proses	ID yang ditetapkan untuk proses oleh sistem operasi.
Namespace PID	ID proses proses dalam namespace PID sekunder selain namespace PID tingkat host. Untuk proses di dalam wadah, itu adalah ID proses yang diamati di dalam wadah.
Memproses ID Pengguna	ID unik pengguna yang mengeksekusi proses.
Proses UUID	ID unik yang ditetapkan untuk proses oleh GuardDuty.
Proses GID	ID proses dari grup proses.
Proses EGID	ID grup yang efektif dari grup proses.
Proses EUID	ID pengguna yang efektif dari proses tersebut.
Nama Pengguna Proses	Nama pengguna yang menjalankan proses.
Waktu Mulai Proses	Waktu ketika proses itu dibuat. Bidang ini dalam format string tanggal UTC (`2023-03-22T19:37:20.168Z`).
Proses yang Dapat Dieksekusi SHA-256	`SHA256`Hash dari proses yang dapat dieksekusi.
Jalur Skrip Proses	Path dari file script yang dieksekusi.
Variabel Lingkungan Proses	Variabel lingkungan tersedia untuk proses. Hanya `LD_PRELOAD` dan `LD_LIBRARY_PATH` dikumpulkan.
Proses Direktori Kerja Saat Ini (PWD)	Presentasikan direktori kerja proses.

Nama bidang	Deskripsi
Proses orang tua	Rincian proses proses induk. Proses induk adalah proses yang menciptakan proses yang diamati.
Argumen Baris Perintah Saat ini, bidang ini terbatas pada versi agen tertentu yang sesuai dengan jenis sumber daya: • Fargate (hanya Amazon ECS) dengan agen GuardDuty keamanan v1.0.0 ke atas. • Instans Amazon EC2 dengan agen GuardDuty keamanan v1.0.0 dan yang lebih baru. • Amazon EKS cluster dengan agen keamanan v1.4.0 dan di atasnya. Untuk informasi selengkapnya, lihat GuardDuty versi rilis agen keamanan.	Command-line argumen yang diberikan pada saat eksekusi proses. Bidang ini mungkin berisi data pelanggan yang sensitif.

Acara kontainer

Peristiwa kontainer mewakili informasi yang terkait dengan aktivitas beban kerja kontainer. Tabel berikut mencakup nama bidang dan deskripsi peristiwa beban kerja kontainer yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Nama Kontainer	Nama wadahnya. Bila tersedia, bidang ini menampilkan nilai label`io.kubernetes.container.name`.
Kontainer UID	ID unik dari kontainer yang ditetapkan oleh runtime kontainer.

Nama bidang	Deskripsi
Runtime Kontainer	Runtime kontainer (seperti `docker` atau`containerd`) digunakan untuk menjalankan kontainer.
ID Gambar Kontainer	ID dari gambar kontainer.
Nama Gambar Kontainer	Nama gambar kontainer.

AWS Fargate (Hanya Amazon ECS) peristiwa tugas

Fargate-Amazon Peristiwa tugas ECS mewakili aktivitas yang terkait dengan tugas Amazon ECS yang berjalan di komputasi Fargate. Tabel berikut mencakup nama bidang dan deskripsi peristiwa ECS-Fargate tugas Amazon yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Nama Sumber Daya Tugas Amazon (ARN)	ARN dari tugas tersebut.
Nama Klaster	Nama cluster Amazon ECS.
Nama Keluarga	Nama keluarga definisi tugas. `family`Ini digunakan sebagai nama untuk definisi tugas yang digunakan untuk meluncurkan tugas.
Nama Layanan	Nama layanan Amazon ECS, jika tugas diluncurkan sebagai bagian dari layanan.
Jenis Peluncuran	Infrastruktur tempat tugas Anda berjalan. Untuk Runtime Monitoring dengan resource type as`ECSCluster` , tipe peluncuran bisa berupa salah satu `EC2` atau`FARGATE`.
CPU	Jumlah unit CPU yang digunakan oleh tugas seperti yang dinyatakan dalam definisi tugas.

Acara pod Kubernetes

Tabel berikut mencakup nama bidang dan deskripsi dari peristiwa pod Kubernetes yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
ID Pod	ID dari pod Kubernetes.
Nama pod	Nama pod Kubernetes.
Ruang Nama Pod	Nama namespace Kubernetes tempat beban kerja Kubernetes berada.
Nama Cluster Kubernetes	Nama cluster Kubernetes.

Acara Sistem Nama Domain (DNS)

Peristiwa Sistem Nama Domain (DNS) mencakup rincian kueri DNS yang dibuat oleh jenis sumber daya Anda dan tanggapan yang sesuai. Tabel berikut mencakup nama bidang dan deskripsi peristiwa DNS yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Jenis Soket	Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, `SOCK_RAW`.
Alamat Keluarga	Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat `AF_INET` digunakan untuk protokol IPv4.
ID Arah	ID dari arah koneksi.
Nomor Protokol	Nomor protokol layer 4 seperti 17 untuk UDP dan 6 untuk TCP.
IP Titik Akhir Jarak Jauh DNS	IP jarak jauh dari koneksi.

Nama bidang	Deskripsi
Port Titik Akhir Jarak Jauh DNS	Nomor port koneksi.
IP Titik Akhir Lokal DNS	IP lokal dari koneksi.
Pelabuhan Titik Akhir Lokal DNS	Nomor port koneksi.
Muatan DNS	Payload paket DNS yang berisi kueri dan tanggapan DNS.

Buka acara

Acara terbuka dikaitkan dengan akses dan modifikasi file. Tabel berikut mencakup nama bidang dan deskripsi peristiwa terbuka yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Filepath	Jalur file yang dibuka dalam acara ini.
Bendera	Menjelaskan mode akses file, seperti read-only, write-only, dan read-write.

Memuat acara modul

Tabel berikut mencakup nama bidang dan deskripsi peristiwa modul beban yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Nama Modul	Nama modul dimuat ke dalam kernel.

Acara Mprotect

Acara Mprotect memberikan informasi tentang perubahan pada pengaturan perlindungan memori dari proses yang berjalan pada sistem yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa Mprotect yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Rentang Alamat	Rentang alamat tempat perlindungan aksesnya dimodifikasi.
Wilayah Memori	Menentukan wilayah ruang alamat proses seperti tumpukan dan heap.
Bendera	Merupakan opsi yang mengontrol perilaku acara ini.

Acara gunung

Mount event memberikan informasi yang terkait dengan pemasangan dan pelepasan sistem file pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa pemasangan yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Target Gunung	Jalur tempat sumber mount dipasang.
Sumber Gunung	Jalur pada host yang dipasang di target mount.
Jenis Sistem File	Merupakan jenis FileSystem yang dipasang.
Bendera	Merupakan opsi yang mengontrol perilaku acara ini.

Tautkan acara

Peristiwa tautan memberikan visibilitas ke dalam aktivitas manajemen tautan sistem file di sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa tautan yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Jalur Tautan	Jalur tempat hard link dibuat.
Jalur Target	Jalur file di mana hard link menunjuk.

Acara Symlink

Acara Symlink memberikan visibilitas ke dalam aktivitas manajemen tautan simbolik sistem file di sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa symlink yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Jalur Tautan	Jalur tempat tautan simbolis dibuat.
Jalur Target	Jalur file di mana tautan simbolik menunjuk.

Acara Dup

Peristiwa Dup memberikan visibilitas ke dalam duplikasi deskriptor file dengan proses yang berjalan pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa dup yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Deskriptor File Lama	Deskriptor file yang mewakili objek file terbuka.
Deskriptor File Baru	Deskriptor file baru yang merupakan duplikat dari deskriptor file lama. Baik deskriptor file lama dan baru mewakili objek file terbuka yang sama.
IP Titik Akhir Jarak Jauh Dup	Alamat IP jarak jauh dari soket jaringan diwakili oleh deskripto r file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.

Nama bidang	Deskripsi
Port Titik Akhir Jarak Jauh Dup	Port jarak jauh dari soket jaringan diwakili oleh deskriptor file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.
IP Titik Akhir Lokal Dup	Alamat IP lokal dari soket jaringan diwakili oleh deskriptor file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.
Pelabuhan Titik Akhir Lokal Dup	Port lokal soket jaringan diwakili oleh deskriptor file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.

Acara peta memori

Tabel berikut mencakup nama bidang dan deskripsi peristiwa peta memori yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Filepath	Jalur file tempat memori dipetakan.

Acara soket

Peristiwa soket memberikan informasi tentang koneksi soket jaringan yang digunakan dalam aktivitas sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa soket yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Keluarga alamat	Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat `AF_INET` digunakan untuk protokol IPv4.
Jenis Soket	Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, `SOCK_RAW`.

Nama bidang	Deskripsi
Nomor protokol	Menentukan protokol tertentu dalam keluarga alamat. Biasanya ada protokol tunggal dalam keluarga alamat. Misalnya, keluarga alamat `AF_INET` hanya memiliki protokol IP.

Connect event

Acara Connect memberikan visibilitas ke dalam koneksi jaringan yang dibuat oleh proses pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa connect yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Keluarga alamat	Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat `AF_INET` digunakan untuk protokol IPv4.
Jenis Soket	Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, `SOCK_RAW`.
Nomor Protokol	Menentukan protokol tertentu dalam keluarga alamat. Biasanya ada protokol tunggal dalam keluarga alamat. Misalnya, keluarga alamat `AF_INET` hanya memiliki protokol IP.
Filepath	Jalur file soket jika keluarga alamat adalah`AF_UNIX`.
IP Titik Akhir Jarak Jauh	IP jarak jauh dari koneksi.
Port Endpoint Jarak Jauh	Nomor port koneksi.
IP Titik Akhir Lokal	IP lokal dari koneksi.
Pelabuhan Endpoint Lokal	Nomor port koneksi.

Memproses acara VM Readv

Proses peristiwa readv VM memberikan visibilitas ke dalam operasi baca yang dilakukan oleh proses di wilayah memori virtual mereka sendiri. Tabel berikut mencakup nama bidang dan deskripsi peristiwa readv VM proses yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Bendera	Merupakan opsi yang mengontrol perilaku acara ini.
Target PID	ID proses dari proses dari mana memori sedang dibaca.
Proses Target UUID	ID unik dari proses target.
Target Jalur yang Dapat Dieksekusi	Jalur absolut dari file eksekusi proses target.

Proses acara VM Writev

Proses peristiwa VM writev memberikan visibilitas ke dalam operasi tulis yang dilakukan oleh proses di wilayah memori virtual mereka sendiri. Tabel berikut mencakup nama bidang dan deskripsi proses VM writev peristiwa yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Bendera	Merupakan opsi yang mengontrol perilaku acara ini.
Target PID	ID proses dari proses dimana memori sedang ditulis.
Proses Target UUID	ID unik dari proses target.
Target Jalur yang Dapat Dieksekusi	Jalur absolut dari file eksekusi proses target.

Process trace (Ptrace) peristiwa

Process trace (Ptrace) system call adalah mekanisme debugging dan tracing yang memungkinkan satu proses (tracer) untuk mengamati dan mengontrol eksekusi proses lain (tracea). Ini memberi pelacak kemampuan untuk memeriksa dan memodifikasi memori, register, dan alur eksekusi proses target.

Peristiwa Ptrace memberikan visibilitas ke dalam penggunaan panggilan sistem ptrace oleh proses yang berjalan pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa ptrace yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Target PID	ID proses dari proses target.
Proses Target UUID	ID unik dari proses target.
Target Jalur yang Dapat Dieksekusi	Jalur absolut dari file eksekusi proses target.
Bendera	Merupakan opsi yang mengontrol perilaku acara ini.

Mengikat acara

Peristiwa mengikat memberikan visibilitas ke dalam pengikatan soket jaringan dengan proses yang berjalan pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa bind yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Alamat Keluarga	Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat `AF_INET` digunakan untuk protokol IPv4.
Jenis soket	Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, `SOCK_RAW`.
Nomor protokol	Nomor protokol layer 4 seperti 17 untuk UDP dan 6 untuk TCP.

Nama bidang	Deskripsi
IP titik akhir lokal	IP lokal dari koneksi.
Port titik akhir lokal	Nomor port koneksi.

Dengarkan acara

Peristiwa mendengarkan memberikan visibilitas ke dalam keadaan mendengarkan soket jaringan, yang menunjukkan apakah soket jaringan siap menerima koneksi masuk atau tidak. Proses yang berjalan pada sumber daya yang dipantau akan menyetel soket jaringan ke status mendengarkan. Tabel berikut mencakup nama bidang dan deskripsi peristiwa mendengarkan yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Alamat Keluarga	Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat `AF_INET` digunakan untuk protokol IPv4.
Jenis soket	Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, `SOCK_RAW`.
Nomor protokol	Nomor protokol layer 4 seperti 17 untuk UDP dan 6 untuk TCP.
IP titik akhir lokal	IP lokal dari koneksi.
Port titik akhir lokal	Nomor port koneksi.

Ganti nama acara

Ganti nama acara memberikan informasi tentang penggantian nama file dan direktori dengan proses yang berjalan pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa ganti nama yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Filepath	Path dari file yang diganti namanya.
Target	Path baru dari file.

Mengatur peristiwa ID pengguna (UID)

Peristiwa set ID pengguna (UID) memberikan visibilitas ke dalam perubahan yang dibuat pada ID pengguna (UID) yang terkait dengan proses yang sedang berjalan pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa UID set yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
EUID baru	ID pengguna baru yang efektif dari proses tersebut.
UID baru	ID pengguna baru dari proses tersebut.

Acara Chmod

Peristiwa Chmod memberikan visibilitas ke dalam perubahan izin (mode) file dan direktori pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa chmod yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Filepath	Path dari file yang memanggil acara ini.
Filemode	Izin akses yang diperbarui untuk file terkait.

Agen hosting repositori Amazon ECR GuardDuty

Bagian berikut mencantumkan repositori Amazon Elastic Container Registry (Amazon ECR) GuardDuty tempat menyimpan agen keamanan yang akan digunakan di sumber daya Amazon EKS, Amazon ECS, dan Amazon EC2 Bottlerocket Anda. ECS-Amazon

Prasyarat untuk Prasyarat untuk akses gambar kontainer mengharuskan Anda memberikan peran eksekusi tugas yang memiliki izin Amazon Elastic Container Registry (Amazon ECR) tertentu. Untuk lebih membatasi izin ini, Anda dapat menambahkan URI repositori Amazon ECR yang menghosting agen untuk sumber daya ECS. GuardDuty Fargate-Amazon

Daftar Isi

- Repositori ECR untuk agen EKS versi 1.16.0 - 1.8.1 (eks.build.2)
- Repositori ECR untuk agen EKS versi 1.8.1 (eks.build.1)
- Repositori ECR untuk agen di GuardDuty AWS Fargate (Hanya Amazon ECS)
- Repositori ECR untuk GuardDuty agen di Bottlerocket ECS-EC2

Repositori ECR untuk agen EKS versi 1.16.0 - 1.8.1 (eks.build.2)

Saat Anda mengaktifkan konfigurasi GuardDuty otomatis untuk Runtime Monitoring untuk EKS, GuardDuty akan menerapkan versi agen ini ke kluster Amazon EKS Anda. Untuk informasi tentang mengaktifkan agen otomatis, lihatMengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS.

Tabel berikut menunjukkan URI repositori Amazon ECR tempat versi agen GuardDuty keamanan`1.16.0.eks.build.2`,,,,, `1.15.0.eks.build.2` `1.11.0.eks.build.2`1.10.0.eks.build.2, `1.9.0.eks.build.2` dan untuk `1.8.0.eks.build.2` Amazon EKS di-host.

Wilayah AWS	URI repositori Amazon ECR
AS Barat (Oregon)	`602401143452.dkr.ecr.us-west-2.amazonaws.com`
	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Eropa (Paris)	`602401143452.dkr.ecr.eu-west-3.amazonaws.com`
	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`

Wilayah AWS	URI repositori Amazon ECR
Asia Pasifik (Mumbai)	602401143452.dkr.ecr.ap-south-1.amazonaws.com
	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asia Pasifik (Hyderabad)	900889452093.dkr.ecr.ap-south-2.amazonaws.com
	618745550137.dkr.ecr.ap-south-2.amazonaws.com
Kanada (Pusat)	602401143452.dkr.ecr.ca-central-1.amazonaws.com
	001188825231.dkr.ecr.ca-central-1.amazonaws.com
Kanada Barat (Calgary)	761377655185.dkr.ecr.ca-west-1.amazonaws.com
	–
Timur Tengah (UAE)	759879836304.dkr.ecr.me-central-1.amazonaws.com
	601769779514.dkr.ecr.me-central-1.amazonaws.com
Eropa (London)	602401143452.dkr.ecr.eu-west-2.amazonaws.com
	109118265657.dkr.ecr.eu-west-2.amazonaws.com
AS Barat (California Utara)	602401143452.dkr.ecr.us-west-1.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
	373421517865.dkr.ecr.us-west-1.amazonaws.com
Timur AS (N. Virginia)	602401143452.dkr.ecr.us-east-1.amazonaws.com
	031903291036.dkr.ecr.us-east-1.amazonaws.com
AS Timur (Ohio)	602401143452.dkr.ecr.us-east-2.amazonaws.com
	591382732059.dkr.ecr.us-east-2.amazonaws.com
Eropa (Irlandia)	602401143452.dkr.ecr.eu-west-1.amazonaws.com
	673884943994.dkr.ecr.eu-west-1.amazonaws.com
Amerika Selatan (Sao Paulo)	602401143452.dkr.ecr.sa-east-1.amazonaws.com
	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Eropa (Stockholm)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Eropa (Frankfurt)	602401143452.dkr.ecr.eu-central-1.amazonaws.com
	409493279830.dkr.ecr.eu-central-1.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
Europe (Zurich)	900612956339.dkr.ecr.eu-central-2.amazonaws.com
	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asia Pasifik (Singapura)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com
	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asia Pasifik (Sydney)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asia Pasifik (Jakarta)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asia Pasifik (Tokyo)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asia Pasifik (Seoul)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia Pasifik (Osaka)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asia Pasifik (Hong Kong)	800184023465.dkr.ecr.ap-east-1.amazonaws.com
	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Middle East (Bahrain) (Middle East (Bahrain))	558608220178.dkr.ecr.me-south-1.amazonaws.com
	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europe (Milan)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Eropa (Spanyol)	455263428931.dkr.ecr.eu-south-2.amazonaws.com
	531047660167.dkr.ecr.eu-south-2.amazonaws.com
Africa (Cape Town)	877085696533.dkr.ecr.af-south-1.amazonaws.com
	379032919888.dkr.ecr.af-south-1.amazonaws.com
Asia Pacific (Melbourne)	491585149902.dkr.ecr.ap-southeast-4.amazonaws.com
	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
Israel (Tel Aviv)	`066635153087.dkr.ecr.il-central-1.amazonaws.com`
	`292660727137.dkr.ecr.il-central-1.amazonaws.com`
Asia Pasifik (Malaysia)	`151610086707.dkr.ecr.ap-southeast-5.amazonaws.com`
Asia Pasifik (Thailand)	`121268973566.dkr.ecr.ap-southeast-7.amazonaws.com`
Meksiko (Tengah)	`730335286997.dkr.ecr.mx-central-1.amazonaws.com`
Asia Pasifik (Taipei)	`533267051163.dkr.ecr.ap-east-2.amazonaws.com`

Repositori ECR untuk agen EKS versi 1.8.1 (eks.build.1)

Bagian ini menyediakan repositori Amazon ECR untuk agen Amazon EKS versi 1.8.1 (v1.8.1-eks-build.1). Jika Anda menggunakan v1.8.1-eks-build.1, GuardDuty rekomendasikan untuk beralih ke versi agen default yang biasanya merupakan versi agen terbaru. Untuk melakukannya, identifikasi agen terbaru dariVersi agen yang dirilis untuk sumber daya Amazon EKS, dan kemudian lakukan langkah-langkahnyaMemperbarui agen keamanan secara manual untuk sumber daya Amazon EKS.

Tabel berikut menunjukkan URI repositori Amazon ECR tempat versi agen GuardDuty keamanan untuk `1.8.1-eks-build.1` Amazon EKS di-host.

Wilayah AWS	URI repositori Amazon ECR
AS Barat (Oregon)	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Eropa (Paris)	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`

Wilayah AWS	URI repositori Amazon ECR
Asia Pasifik (Mumbai)	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asia Pasifik (Hyderabad)	618745550137.dkr.ecr.ap-south-2.amazonaws.com
Kanada (Pusat)	001188825231.dkr.ecr.ca-central-1.amazonaws.com
Timur Tengah (UAE)	601769779514.dkr.ecr.me-central-1.amazonaws.com
Eropa (London)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
AS Barat (California Utara)	373421517865.dkr.ecr.us-west-1.amazonaws.com
Timur AS (N. Virginia)	031903291036.dkr.ecr.us-east-1.amazonaws.com
AS Timur (Ohio)	591382732059.dkr.ecr.us-east-2.amazonaws.com
Eropa (Irlandia)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
Amerika Selatan (Sao Paulo)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Eropa (Stockholm)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Eropa (Frankfurt)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Europe (Zurich)	718440343717.dkr.ecr.eu-central-2.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
Asia Pasifik (Singapura)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asia Pasifik (Sydney)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asia Pasifik (Jakarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asia Pasifik (Tokyo)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asia Pasifik (Seoul)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia Pasifik (Osaka)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asia Pasifik (Hong Kong)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Middle East (Bahrain) (Middle East (Bahrain))	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europe (Milan)	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Eropa (Spanyol)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
Africa (Cape Town)	379032919888.dkr.ecr.af-south-1.amazonaws.com
Asia Pacific (Melbourne)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
Israel (Tel Aviv)	292660727137.dkr.ecr.il-central-1.amazonaws.com

Repositori ECR untuk agen di GuardDuty AWS Fargate (Hanya Amazon ECS)

Sebagai prasyarat untuk menggunakan Runtime Monitoring untuk Amazon ECS-Fargate, Anda harus. Prasyarat untuk akses gambar kontainer Gambar wadah sespan GuardDuty agen disimpan di Amazon ECR, dengan lapisan gambarnya disimpan di Amazon S3. Untuk informasi selengkapnya, lihat Menyebarkan agen keamanan ke Amazon ECS di Fargate.

Tabel berikut menunjukkan repositori Amazon ECR yang menjadi tuan rumah GuardDuty agen untuk (hanya AWS Fargate Amazon ECS) untuk masing-masing. Wilayah AWS

Wilayah AWS	URI repositori Amazon ECR
AS Barat (Oregon)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate`
Eropa (Paris)	`665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate`
Asia Pasifik (Mumbai)	`251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asia Pasifik (Hyderabad)	`950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate`
Kanada (Pusat)	`354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Timur Tengah (UAE)	`000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate`

Wilayah AWS	URI repositori Amazon ECR
Eropa (London)	892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate
AS Barat (California Utara)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate
Timur AS (N. Virginia)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate
AS Timur (Ohio)	307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate
Eropa (Irlandia)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate
Amerika Selatan (Sao Paulo)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate
Eropa (Stockholm)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate
Eropa (Frankfurt)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate
Europe (Zurich)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate

Wilayah AWS	URI repositori Amazon ECR
Asia Pasifik (Singapura)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Sydney)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Jakarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Tokyo)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Seoul)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Osaka)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
Middle East (Bahrain) (Middle East (Bahrain))	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guarddduty-agent-fargate
Europe (Milan)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guarddduty-agent-fargate

Wilayah AWS	URI repositori Amazon ECR
Eropa (Spanyol)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate
Africa (Cape Town)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacific (Melbourne)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate
Israel (Tel Aviv)	870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Malaysia)	156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Thailand)	054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-fargate
Kanada Barat (Calgary)	339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-fargate
Meksiko (Tengah)	311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Taipei)	259886477082.dkr.ecr.ap-east-2.amazonaws.com/aws-guardduty-agent-fargate

Repositori ECR untuk GuardDuty agen di Bottlerocket ECS-EC2

Pada instans Bottlerocket ECS-Amazon Amazon EC2, agen keamanan berjalan GuardDuty sebagai wadah host. Gambar wadah agen di-host di Amazon ECR. Untuk informasi tentang prasyarat termasuk konektivitas jaringan dan izin IAM yang diperlukan, lihat. Prasyarat untuk dukungan Bottlerocket ECS-EC2 Profil instans harus menyertakan `AmazonSSMManagedInstanceCore` dan kebijakan yang `AmazonEC2ContainerRegistryReadOnly` dikelola.

Tabel berikut menunjukkan repositori Amazon ECR yang menjadi tuan rumah agen untuk instans GuardDuty Bottlerocket Amazon ECS-Amazon EC2 untuk masing-masing. Wilayah AWS

Wilayah AWS	URI repositori Amazon ECR
Timur AS (N. Virginia)	`593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
AS Timur (Ohio)	`307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
AS Barat (California Utara)	`684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
US West (Oregon)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europe (Ireland)	`694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Eropa (London)	`892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`

Wilayah AWS	URI repositori Amazon ECR
Europe (Paris)	`665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Eropa (Frankfurt)	`323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europe (Zurich)	`529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Eropa (Stockholm)	`591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guarddduty-agent-ecs-ec2`
Europe (Milan)	`266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guarddduty-agent-ecs-ec2`
Eropa (Spanyol)	`919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guarddduty-agent-ecs-ec2`
Asia Pasifik (Tokyo)	`533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Asia Pasifik (Seoul)	`914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Asia Pasifik (Osaka)	`273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-ecs-ec2`

Wilayah AWS	URI repositori Amazon ECR
Asia Pasifik (Singapura)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asia Pasifik (Sydney)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asia Pasifik (Jakarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asia Pasifik (Melbourne)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asia Pasifik (Mumbai)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guarduty-agent-ecs-ec2
Asia Pasifik (Hyderabad)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guarduty-agent-ecs-ec2
Asia Pasifik (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Kanada (Pusat)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Kanada Barat (Calgary)	339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-ecs-ec2

Wilayah AWS	URI repositori Amazon ECR
South America (Sao Paulo)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Timur Tengah (Bahrain)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Middle East (UAE)	000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Africa (Cape Town)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Israel (Tel Aviv)	870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asia Pasifik (Malaysia)	156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asia Pasifik (Thailand)	054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-ecs-ec2
Meksiko (Tengah)	311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asia Pasifik (Taipei)	259886477082.dkr.ecr.ap-east-2.amazonaws.com/aws-guardduty-agent-ecs-ec2

Dua agen keamanan pada host yang mendasari yang sama

Instans Amazon EC2 dapat mendukung beberapa jenis beban kerja. Saat Anda mengonfigurasi agen keamanan otomatis di instans Amazon EC2, instans EC2 yang sama mungkin memiliki agen keamanan lain melalui EKS.

Gambaran umum

Pertimbangkan skenario di mana Anda telah mengaktifkan Runtime Monitoring. Sekarang, Anda mengaktifkan agen otomatis untuk Amazon EKS melalui GuardDuty. Anda juga telah mengaktifkan agen otomatis untuk Amazon EC2. Mungkin saja host dasar yang sama diinstal dengan dua agen keamanan - satu untuk Amazon EKS dan yang lainnya untuk Amazon EC2. Hal ini dapat mengakibatkan dua agen keamanan berjalan di dalam host yang sama, mengumpulkan peristiwa runtime dan mengirimkannya ke GuardDuty, dan berpotensi menghasilkan temuan duplikat.

Dampak

- Ketika ada lebih dari satu agen keamanan yang berjalan pada host yang sama, akun Anda mungkin mengalami dua kali lipat jumlah kebutuhan pemrosesan CPU dan memori. Untuk informasi tentang CPU dan batas memori untuk setiap jenis sumber daya, lihat Prasyarat sumber daya tersebut.
- GuardDuty telah merancang fitur Runtime Monitoring sedemikian rupa sehingga meskipun ada tumpang tindih dua agen keamanan yang mengumpulkan peristiwa runtime dari host dasar yang sama, akun Anda hanya akan dikenakan biaya untuk satu aliran peristiwa runtime.

Bagaimana GuardDuty menangani banyak agen

GuardDuty mendeteksi ketika dua agen keamanan berjalan pada host yang sama dan menunjuk hanya satu dari mereka untuk menjadi agen keamanan yang secara aktif mengumpulkan peristiwa runtime. Agen kedua akan mengkonsumsi sumber daya sistem minimum untuk mencegah dampak apa pun terhadap kinerja aplikasi Anda.

GuardDuty mempertimbangkan skenario berikut:

- Ketika instans EC2 berada di bawah lingkup agen keamanan Amazon EKS dan Amazon EC2, agen keamanan EKS diprioritaskan. Ini hanya akan berlaku ketika Anda menggunakan agen keamanan v1.1.0 atau lebih tinggi untuk Amazon EC2. Versi agen yang lebih lama akan

terus berjalan dan mengumpulkan peristiwa runtime karena versi agen yang lebih lama tidak terpengaruh oleh prioritas.

- Ketika Amazon EKS dan Amazon EC2 telah GuardDuty mengelola agen keamanan dan instans Amazon EC2 Anda juga dikelola SSM, kedua agen keamanan akan dipasang di tingkat host. Setelah agen diinstal, GuardDuty putuskan agen keamanan mana yang akan terus berjalan. Ketika kedua agen keamanan berjalan, akhirnya hanya satu dari mereka yang akan mengumpulkan acara runtime.
- Ketika agen keamanan yang terkait dengan EC2 dan EKS berjalan pada saat yang sama, GuardDuty mungkin menghasilkan temuan duplikat selama periode tumpang tindih saja.

  Ini bisa terjadi ketika:

  - Agen keamanan untuk EC2 dan EKS dikonfigurasi melalui GuardDuty (secara otomatis), atau
  - Sumber daya Amazon EKS Anda memiliki agen keamanan otomatis.
- Ketika agen keamanan EKS sudah berjalan, jika Anda menerapkan agen keamanan EC2 secara manual pada host dasar yang sama dan memenuhi semua prasyarat, GuardDuty mungkin tidak menginstal agen keamanan kedua.

Pemantauan Runtime EKS di GuardDuty

EKS Runtime Monitoring menyediakan cakupan deteksi ancaman runtime untuk node dan container Amazon Elastic Kubernetes Service (Amazon EKS) di lingkungan Anda. AWS EKS Runtime Monitoring menggunakan agen GuardDuty keamanan yang menambahkan visibilitas runtime ke beban kerja EKS individual, misalnya, akses file, eksekusi proses, dan koneksi jaringan. Agen GuardDuty keamanan membantu GuardDuty mengidentifikasi kontainer tertentu dalam kluster EKS Anda yang berpotensi dikompromikan. Ini juga dapat mendeteksi upaya untuk meningkatkan hak istimewa dari wadah individu ke host EC2 yang mendasarinya, dan lingkungan yang lebih luas. AWS

Dengan ketersediaan Runtime Monitoring, GuardDuty telah mengkonsolidasikan pengalaman konsol untuk EKS Runtime Monitoring menjadi Runtime Monitoring. GuardDuty tidak akan memigrasikan pengaturan Pemantauan Runtime EKS Anda atas nama Anda secara otomatis. Ini membutuhkan tindakan di akhir Anda. Jika Anda ingin terus menggunakan hanya EKS Runtime Monitoring, Anda dapat menggunakan API atau AWS CLI untuk memeriksa dan memperbarui status konfigurasi yang ada untuk EKS Runtime Monitoring. Namun, GuardDuty rekomendasikan Bermigrasi dari Pemantauan Runtime EKS ke Pemantauan Runtime dan gunakan Runtime Monitoring untuk memantau kluster Amazon EKS Anda.

Topik

- Mengkonfigurasi EKS Runtime Monitoring untuk lingkungan multi-akun (API)
- Mengkonfigurasi EKS Runtime Monitoring untuk akun mandiri (API)
- Bermigrasi dari Pemantauan Runtime EKS ke Pemantauan Runtime

Mengkonfigurasi EKS Runtime Monitoring untuk lingkungan multi-akun (API)

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan EKS Runtime Monitoring untuk akun anggota, dan mengelola manajemen GuardDuty agen untuk kluster EKS milik akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat Mengelola beberapa akun.

Mengkonfigurasi EKS Runtime Monitoring untuk akun administrator yang didelegasikan GuardDuty

Bagian ini menyediakan langkah-langkah untuk mengonfigurasi EKS Runtime Monitoring dan mengelola agen GuardDuty keamanan untuk kluster EKS yang termasuk dalam akun administrator yang didelegasikan GuardDuty .

Berdasarkan pendekatan diMenyebarkan agen keamanan ke Amazon EKS, Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Jalankan updateDetectorAPI dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama `features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai`ENABLED`. Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`ENABLED`.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nil ai adalah `GuardDutyManaged` -. `false` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	3. **Note** Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel `EKS_RUNTIME_MONITORING` ke`ENABLED`; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. `STATUS` Jalankan updateDetectorAPI dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama `features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai`ENABLED`. Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`ENABLED`. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantauan. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	features '[{"Name" : "EKS_RUNTIME_MONIT ORING", "Status" : " *ENABLED*", "Addition alConfiguration" : [{"Name" : "EKS_ADDO N_MANAGEMENT", "Status" : " *ENABLED*"}] }]'

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda sertakan dalam pemantauan. Pasangan kunci-nilai adalah `GuardDutyManaged` -. `true` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *`ec2:CreateTags`* dengan`eks:TagResource` . • Ganti *`ec2:DeleteTags`* dengan`eks:UntagResource` . • Ganti *`access-project`* dengan `GuardDutyManaged` • Ganti *`123456789012`* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Jalankan updateDetectorAPI dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	`features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai`ENABLED`. Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`DISABLED`. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan - pair. `GuardDutyManaged true` Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Mengelola agen keamanan secara manual	1. Jalankan updateDetectorAPI dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama `features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai`ENABLED`. Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`DISABLED`. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'` 2. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Auto-enable EKS Runtime Monitoring untuk semua akun anggota

Bagian ini mencakup langkah-langkah untuk mengaktifkan EKS Runtime Monitoring dan mengelola agen keamanan untuk semua akun anggota. Ini termasuk akun GuardDuty administrator yang didelegasikan, akun anggota yang ada, dan akun baru yang bergabung dengan organisasi.

Berdasarkan pendekatan diMenyebarkan agen keamanan ke Amazon EKS, Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID* Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. detectorId Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING danEKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'` **Note** Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nilai adalah `GuardDuty Managed -. false` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa`Principal Arn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel `EKS_RUNTIME_MONITORING` keENABLED; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. `STATUS`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya

Jalankan updateDetectorAPI dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama `features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai`ENABLED`.

Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`ENABLED`.

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantauan.

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan`EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --account-
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM
ENT", "Status" : " ENABLED"}] }]'
```

> **Note**
>
> Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda sertakan dalam pemantauan. Pasangan kunci-nilai adalah `GuardDuty Managed -. true` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipal Arn : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Jalankan updateDetectorAPI dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai EKS_RUNTIME_MONITORING dan status sebagaiENABLED. Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan - pair. `GuardDutyManaged true`

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan`EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --account-
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM
ENT", "Status" : " DISABLED"}] }]'
```

> **Note**
>
> Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Mengelola agen keamanan secara manual	1. Jalankan updateDetectorAPI dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama `features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai`ENABLED`. Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`DISABLED`. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] } ]'` 2. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Mengkonfigurasi EKS Runtime Monitoring untuk semua akun anggota aktif yang ada

Bagian ini mencakup langkah-langkah untuk mengaktifkan EKS Runtime Monitoring dan mengelola agen GuardDuty keamanan untuk akun anggota aktif yang ada di organisasi Anda.

Berdasarkan pendekatan diMenyebarkan agen keamanan ke Amazon EKS, Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID* Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`ENABLED`. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'` **Note** Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi. Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nilai adalah `GuardDuty Managed -. false` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipal Arn : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel EKS_RUNTIME_MONITORING keENABLED; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. STATUS

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID* Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`ENABLED`. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantauan. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` **Note** Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda sertakan dalam pemantauan. Pasangan kunci-nilai adalah `GuardDuty Managed -. true` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipal Arn : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID* Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan - pair. `GuardDutyManaged true`

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan`EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --account-
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM
ENT", "Status" : " DISABLED"}] }]'
```

> **Note**
>
> Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Mengelola agen keamanan secara manual	1. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID* Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`DISABLED`. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] } ]'` 2. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Auto-enable EKS Runtime Monitoring untuk anggota baru

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan EKS Runtime Monitoring secara otomatis dan memilih pendekatan untuk cara mengelola agen GuardDuty keamanan untuk akun baru yang bergabung dengan organisasi Anda.

Berdasarkan pendekatan diMenyebarkan agen keamanan ke Amazon EKS, Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan operasi UpdateOrganizationConfigurationAPI menggunakan akun Anda sendiri. *detector ID* Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`ENABLED`. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan `EKS_ADDON_MANAGEMENT` untuk satu akun. Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	`--autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'` Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nil ai adalah `GuardDutyManaged` -. `false` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	3. **Note** Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel `EKS_RUNTIME_MONITORING` ke`ENABLED`; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. `STATUS` Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan operasi UpdateOrganizationConfigurationAPI menggunakan akun Anda sendiri. *`detector ID`* Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`ENABLED`. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantauan. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan `EKS_ADDON_MANAGEMENT` untuk satu akun. Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'` Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda sertakan dalam pemantauan. Pasangan kunci-nilai adalah `GuardDutyManaged` -. `true` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan operasi

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	UpdateOrganizationConfigurationAPI menggunakan akun Anda sendiri. *detector ID* Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan - pair. GuardDutyManaged true Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. detectorId Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT untuk satu akun. Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. detectorId `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Mengelola agen keamanan secara manual	1. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan operasi UpdateOrganizationConfigurationAPI menggunakan akun Anda sendiri. *detector ID* Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`DISABLED`. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan `EKS_ADDON_MANAGEMENT` untuk satu akun. Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'` Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya. 2. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Aktifkan EKS Runtime Monitoring untuk akun anggota aktif individu

Bagian ini mencakup langkah-langkah untuk mengonfigurasi EKS Runtime Monitoring dan mengelola agen keamanan untuk akun anggota aktif individu.

Berdasarkan pendekatan diMenyebarkan agen keamanan ke Amazon EKS, Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID* Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`ENABLED`. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'` **Note** Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi. Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nil ai adalah `GuardDutyManaged` -. `false` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya

3.

> **Note**
>
> Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel `EKS_RUNTIME_MONITORING` ke`ENABLED`; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. `STATUS`

Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *`detector ID`*

Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`ENABLED`.

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantaua n.

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.a ws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan`EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --
detector-id 12abc34d567e8fa901bc2d34e56
789f0 --account-ids 111122223333 --feature
```

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya

```
s '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "ENABLED", "AdditionalConfigu
ration" : [{"Name" : "EKS_ADDON_MANAGEMENT",
 "Status" : "ENABLED"}] }]'
```

> **Note**
>
> Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda sertakan dalam pemantauan. Pasangan kunci-nilai adalah `GuardDutyManaged` -. `true` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID* Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan - pair. GuardDutyManaged true Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. detectorId Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkanEKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] }]'` **Note** Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Mengelola agen keamanan secara manual	1. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID* Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. detectorId Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkanEKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] } ]'` 2. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Mengkonfigurasi EKS Runtime Monitoring untuk akun mandiri (API)

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat Mengkonfigurasi EKS Runtime Monitoring untuk lingkungan multi-akun (API).

Setelah Anda mengaktifkan Runtime Monitoring, pastikan untuk menginstal agen GuardDuty keamanan melalui konfigurasi otomatis atau penerapan manual. Sebagai bagian dari menyelesaikan semua langkah yang tercantum dalam prosedur berikut, pastikan untuk menginstal agen keamanan.

Berdasarkan pendekatan diMenyebarkan agen keamanan ke Amazon EKS, Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	1. Jalankan updateDetectorAPI dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama `features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai`ENABLED`. Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`ENABLED`. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. 2. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	`features '[{"Name" : "EKS_RUNTIME_MONIT ORING", "Status" : " ENABLED", "Addition alConfiguration" : [{"Name" : "EKS_ADDO N_MANAGEMENT", "Status" : " ENABLED"}] }]'`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nilai adalah `GuardDutyManaged` -. `false` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* dengan `eks:TagResource` . • Ganti *ec2:DeleteTags* dengan `eks:UntagResource` . • Ganti *access-project* dengan `GuardDutyManaged` • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	3. **Note** Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel `EKS_RUNTIME_MONITORING` ke`ENABLED`; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. `STATUS` Jalankan updateDetectorAPI dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama `features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai`ENABLED`. Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`ENABLED`. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantauan. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	`features '[{"Name" : "EKS_RUNTIME_MONIT ORING", "Status" : " ENABLED", "Addition alConfiguration" : [{"Name" : "EKS_ADDO N_MANAGEMENT", "Status" : "  ENABLED"}] }]'`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda sertakan dalam pemantauan. Pasangan kunci-nilai adalah `GuardDutyManaged` -. `true` Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti *ec2:CreateTags* denganeks:TagResource . • Ganti *ec2:DeleteTags* denganeks:UntagResource . • Ganti *access-project* dengan GuardDutyManaged • Ganti *123456789012* dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa`PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Jalankan updateDetectorAPI dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
	`features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai`ENABLED`. Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`DISABLED`. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan - pair. `GuardDutyManaged true` Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'`

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-langkahnya
Mengelola agen keamanan secara manual	1. Jalankan updateDetectorAPI dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama `features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai`ENABLED`. Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as`DISABLED`. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId` Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan`EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'` 2. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk klaster Amazon EKS.

Bermigrasi dari Pemantauan Runtime EKS ke Pemantauan Runtime

Dengan peluncuran GuardDuty Runtime Monitoring, cakupan deteksi ancaman telah diperluas ke wadah Amazon ECS dan instans Amazon EC2. Pengalaman EKS Runtime Monitoring kini telah dikonsolidasikan ke dalam Runtime Monitoring. Anda dapat mengaktifkan Runtime Monitoring dan

mengelola agen GuardDuty keamanan individual untuk setiap jenis sumber daya (instans Amazon EC2, cluster Amazon ECS, dan klaster Amazon EKS) yang ingin Anda pantau perilaku runtime.

GuardDuty telah mengkonsolidasikan pengalaman konsol untuk EKS Runtime Monitoring ke Runtime Monitoring. GuardDuty merekomendasikan Memeriksa status konfigurasi EKS Runtime Monitoring danBermigrasi dari Pemantauan Runtime EKS ke Pemantauan Runtime.

Sebagai bagian dari migrasi ke Runtime Monitoring, pastikan untuk. Nonaktifkan Pemantauan Runtime EKS Ini penting karena jika nanti Anda memilih untuk menonaktifkan Runtime Monitoring dan Anda tidak menonaktifkan EKS Runtime Monitoring, Anda akan terus mengeluarkan biaya penggunaan untuk EKS Runtime Monitoring.

Untuk bermigrasi dari EKS Runtime Monitoring ke Runtime Monitoring

1. GuardDuty Konsol mendukung EKS Runtime Monitoring sebagai bagian dari Runtime Monitoring.

   Anda dapat mulai menggunakan Runtime Monitoring oleh Memeriksa status konfigurasi EKS Runtime Monitoring organisasi dan akun Anda.

   Pastikan untuk tidak menonaktifkan EKS Runtime Monitoring sebelum mengaktifkan Runtime Monitoring. Jika Anda menonaktifkan EKS Runtime Monitoring, manajemen add-on Amazon EKS juga akan dinonaktifkan. Lanjutkan dengan langkah-langkah berikut dalam urutan yang tercantum.
2. Pastikan Anda memenuhi semuaPrasyarat untuk mengaktifkan Pemantauan Runtime.
3. Aktifkan Runtime Monitoring dengan mereplikasi pengaturan konfigurasi organisasi yang sama untuk Runtime Monitoring seperti yang Anda miliki untuk EKS Runtime Monitoring. Untuk informasi selengkapnya, lihat Mengaktifkan Runtime Monitoring.
   - Jika Anda memiliki akun mandiri, Anda harus mengaktifkan Runtime Monitoring.

     Jika agen GuardDuty keamanan Anda sudah digunakan, pengaturan yang sesuai akan direplikasi secara otomatis dan Anda tidak perlu mengonfigurasi pengaturan lagi.
   - Jika Anda memiliki organisasi dengan pengaturan auto-enablement, pastikan untuk mereplikasi pengaturan auto-enablement yang sama untuk Runtime Monitoring.
   - Jika Anda memiliki organisasi dengan pengaturan yang dikonfigurasi untuk akun anggota aktif yang ada secara individual, pastikan untuk mengaktifkan Runtime Monitoring dan mengonfigurasi agen GuardDuty keamanan untuk anggota ini secara individual.
4. Setelah Anda memastikan bahwa pengaturan Runtime Monitoring dan agen GuardDuty keamanan sudah benar, nonaktifkan EKS Runtime Monitoring dengan menggunakan API atau perintah. AWS CLI

5. (Opsional) jika Anda ingin membersihkan sumber daya apa pun yang terkait dengan agen GuardDuty keamanan, lihatMenonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Jika Anda ingin terus menggunakan EKS Runtime Monitoring tanpa mengaktifkan Runtime Monitoring, lihat. Pemantauan Runtime EKS di GuardDuty Berdasarkan kasus penggunaan Anda, pilih langkah-langkah untuk mengonfigurasi EKS Runtime Monitoring untuk akun mandiri atau untuk beberapa akun anggota.

Memeriksa status konfigurasi EKS Runtime Monitoring

Gunakan API atau AWS CLI perintah berikut untuk memeriksa status konfigurasi EKS Runtime Monitoring yang ada.

Untuk memeriksa status konfigurasi EKS Runtime Monitoring yang ada di akun Anda

- Jalankan GetDetectoruntuk memeriksa status konfigurasi akun Anda sendiri.
- Atau, Anda dapat menjalankan perintah berikut dengan menggunakan AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

  Pastikan untuk mengganti ID detektor Wilayah Anda Akun AWS dan saat ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Untuk memeriksa status konfigurasi EKS Runtime Monitoring yang ada untuk organisasi Anda (hanya sebagai akun GuardDuty administrator yang didelegasikan)

- Jalankan DescribeOrganizationConfigurationuntuk memeriksa status konfigurasi organisasi Anda.

  Atau, Anda dapat menjalankan perintah berikut menggunakan AWS CLI:

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

  Pastikan untuk mengganti ID detektor dengan ID detektor akun GuardDuty administrator yang didelegasikan dan Wilayah dengan Wilayah Anda saat ini. Untuk menemukan akun Anda dan

Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Menonaktifkan EKS Runtime Monitoring setelah bermigrasi ke Runtime Monitoring

Setelah Anda memastikan bahwa pengaturan yang ada untuk akun atau organisasi Anda telah direplikasi ke Runtime Monitoring, Anda dapat menonaktifkan EKS Runtime Monitoring.

Untuk menonaktifkan EKS Runtime Monitoring

- Untuk menonaktifkan EKS Runtime Monitoring di akun Anda sendiri

  Jalankan UpdateDetectorAPI dengan regional Anda sendiri*detector-id*.

  Atau, Anda dapat menggunakan AWS CLI perintah berikut. Ganti *12abc34d567e8fa901bc2d34e56789f0* dengan regional Anda sendiri*detector-id*.

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
  ```

- Untuk menonaktifkan EKS Runtime Monitoring untuk akun anggota di organisasi Anda

  Jalankan UpdateMemberDetectorsAPI dengan regional *detector-id* dari akun GuardDuty administrator yang didelegasikan dari organisasi.

  Atau, Anda dapat menggunakan AWS CLI perintah berikut. Ganti *12abc34d567e8fa901bc2d34e56789f0* dengan regional *detector-id* akun GuardDuty administrator yang didelegasikan dari organisasi dan *111122223333* dengan Akun AWS ID akun anggota yang ingin Anda nonaktifkan fitur ini.

  ```
  aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
   --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
   "Status" : "DISABLED"}]'
  ```

- Untuk memperbarui EKS Runtime Monitoring, aktifkan pengaturan otomatis untuk organisasi Anda

  Lakukan langkah berikut hanya jika Anda telah mengonfigurasi pengaturan pengaktifan otomatis EKS Runtime Monitoring ke akun anggota baru (`NEW`) atau semua (`ALL`) di organisasi. Jika Anda sudah mengonfigurasinya sebagai`NONE`, maka Anda dapat melewati langkah ini.

> **Note**
>
> Menyetel konfigurasi pengaktifan otomatis EKS Runtime Monitoring `NONE` berarti bahwa EKS Runtime Monitoring tidak akan diaktifkan secara otomatis untuk akun anggota yang ada atau ketika akun anggota baru bergabung dengan organisasi Anda.

Jalankan UpdateOrganizationConfigurationAPI dengan regional *`detector-id`* dari akun GuardDuty administrator yang didelegasikan dari organisasi.

Atau, Anda dapat menggunakan AWS CLI perintah berikut. Ganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan regional *`detector-id`* dari akun GuardDuty administrator yang didelegasikan dari organisasi. Ganti *`EXISTING_VALUE`* dengan konfigurasi Anda saat ini untuk mengaktifkan otomatis GuardDuty.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

GuardDuty versi rilis agen keamanan

GuardDuty merilis versi agen yang diperbarui dari waktu ke waktu. Ketika GuardDuty mengelola agen secara otomatis, GuardDuty dirancang untuk memperbarui agen atas nama Anda. Saat mengelola agen secara manual, Anda bertanggung jawab untuk memperbarui versi agen untuk jenis sumber daya Anda — instans Amazon EC2, kluster Amazon ECS, dan kluster Amazon EKS.

Bagian berikut menyediakan versi rilis agen GuardDuty keamanan dan catatan rilis terkait untuk semua jenis sumber daya yang didukung.

Topik

- GuardDuty versi agen keamanan untuk instans Amazon EC2
- GuardDuty versi agen keamanan untuk Amazon ECS-EC2 Bottlerocket
- GuardDuty versi agen keamanan untuk AWS Fargate (Hanya Amazon ECS)
- GuardDuty versi agen keamanan untuk sumber daya Amazon EKS
- Sumber daya tambahan - langkah selanjutnya

GuardDuty versi agen keamanan untuk instans Amazon EC2

Tabel berikut menunjukkan riwayat versi rilis untuk agen GuardDuty keamanan untuk Amazon EC2.

Versi distributor SSM	Versi agen	Catatan rilis	Tanggal ketersediaan
v1.17.1	v1.17.1	Menambahkan dukungan untuk Kernel 7.2. Saat startup, agen mendeteksi jenis GuardDuty konektivitas dan mencoba terhubung ke titik akhir guardduty-data-v2 melalui link-local. Pembaruan fitur keamanan umum.	Sep 9, 2026
v1.16.0	v1.16.0	Menambahkan dukungan untuk Kernel 6.19, 7.0, 7.1. Menambahkan dukungan untuk Ubuntu 26.04, Debian 13, RedHat 10.2, CentOS Stream 10, Rocky Linux 10.1, Fedora 43, dan Fedora 44. Untuk daftar semua distribusi OS terverifikasi untuk sumber daya Amazon EC2, lihat.	Juli 17, 2026

Versi distributor SSM	Versi agen	Catatan rilis	Tanggal ketersediaan
		Validasi persyaratan arsitektur Pembaruan fitur keamanan umum.	
v1.15.0	v1.15.0	Kemampuan agen baru untuk mendukung pengumpulan peristiwa yang dioptimalkan, memungkinkan penyebaran filter yang lebih cepat dan kecepatan deteksi yang lebih baik. Pembaruan fitur keamanan umum.	14 Mei 2026

Versi distributor SSM	Versi agen	Catatan rilis	Tanggal ketersediaan
v1.9.2	v1.9.2	Menambahkan dukungan untuk Kernel 6.15, 6.16, 6.17, 6.18. Menambahkan dukungan untuk Alma Linux 9, Alma Linux 10 dan SUSE Linux Enterprise Server 16. Untuk daftar semua distribusi OS terverifikasi untuk sumber daya Amazon EC2, lihat. Validasi persyaratan arsitektur	Februari 24, 2026
v1.9.1	v1.9.1	Penyetelan kinerja umum dan pembaruan fitur keamanan.	Nov 10, 2025
v1.9.0	v1.9.0	Penyetelan dan peningkatan kinerja umum.	Oktober 23, 2025
v1.8.0	v1.8.0	Penyetelan dan peningkatan kinerja umum.	Agustus 12, 2025
v1.7.2	v1.7.1	Peningkatan dukungan untuk instalasi agen lokal untuk distribusi Linux berbasis RPM.	Juli 23, 2025

Versi distributor SSM	Versi agen	Catatan rilis	Tanggal ketersediaan
v1.7.1	1.7.1	Ditambahkan dukungan untuk Fedora 40 dan Fedora 41. Untuk daftar semua distribusi OS terverifikasi untuk sumber daya Amazon EC2, lihat. Validasi persyaratan arsitektur Penyetelan dan peningkatan kinerja umum.	Juni 03, 2025
v1.7.0	v1.7.0	Menambahkan dukungan untuk Oracle Linux versi 8.9 dan 9.3, dan Rocky Linux versi 9.5. Untuk daftar semua distribusi OS terverifikasi untuk sumber daya Amazon EC2, lihat. Validasi persyaratan arsitektur Resolusi ID kontainer yang ditingkatkan. Penyetelan dan peningkatan kinerja umum.	April 03, 2025
v1.6.0	v1.6.0	Penyetelan dan peningkatan kinerja umum.	Februari 6, 2025

Versi distributor SSM	Versi agen	Catatan rilis	Tanggal ketersediaan
v1.5.0	v1.5.0	Menambahkan dukungan untuk CentOS Stream 9.0, RedHat 9.4, Fedora 34.0, dan Ubuntu 24.04. Support untuk instance ARM untuk `.../MetadataDNSRebind` temuan. Penyetelan dan peningkatan kinerja umum.	November 20, 2024
v1.3.1	v1.3.1	Support untuk resolver DNS kustom.	September 12, 2024
v1.3.0	v1.3.0	Penyetelan dan peningkatan kinerja umum. Termasuk dukungan untuk menangkap sinyal keamanan tambahan untuk masa depanGuardDuty Jenis penemuan Runtime Monitoring.	Agustus 19, 2024

Versi distributor SSM	Versi agen	Catatan rilis	Tanggal ketersediaan
v1.2.0	v1.2.0	Mendukung distribusi OS Ubuntu 20.04, Ubuntu 22.04, Debian 11, dan Debian 12. Mendukung kernel 6.5 dan 6.8. Penyetelan dan peningkatan kinerja umum.	Juni 13, 2024
v1.1.0	v1.1.0	Mendukung konfigurasi agen GuardDuty otomatis dalam Runtime Monitoring untuk instans Amazon EC2. Mendukung sinyal keamanan baru dan temuan yang dirilis dengan pengumuman ketersediaan umum Runtime Monitoring untuk instans EC2. Penyetelan dan peningkatan kinerja umum.	26 Maret 2024
v1.0.2	v1.0.2	Mendukung AMI Amazon ECS terbaru.	Februari 2, 2024

Versi distributor SSM	Versi agen	Catatan rilis	Tanggal ketersediaan
v1.0.1	v1.0.1	Versi agen yang dirilis sebelum v1.0.2 tidak kompatibel dengan Amazon ECS AMI yang diluncurkan setelah 31 Januari 2024. Penyetelan dan peningkatan kinerja umum.	23 Januari 2024
v1.0.0	v1.0.0	Pelepasan awal instalasi RPM. Versi agen yang dirilis sebelum v1.0.2 tidak kompatibel dengan Amazon ECS AMI yang diluncurkan setelah 31 Januari 2024.	26 November 2023

GuardDuty versi agen keamanan untuk Amazon ECS-EC2 Bottlerocket

Tabel berikut menunjukkan riwayat versi rilis untuk agen GuardDuty keamanan untuk instans Amazon ECS-EC2 Bottlerocket. Agen berjalan sebagai wadah host di Bottlerocket dan versi ECS-3 AMI yang ECS-2 dioptimalkan ke atas. `v1.62.1`

Versi Distributor SSM	Versi agen	Catatan rilis	Tanggal ketersediaan
v1.17.1	v1.17.1	Menambahkan dukungan untuk Kernel 7.2.	Sep 9, 2026

Versi Distributor SSM	Versi agen	Catatan rilis	Tanggal ketersediaan
		Saat startup, agen mendeteksi jenis GuardDuty konektivitas dan mencoba terhubung ke titik akhir guardduty-data-v2 melalui link-local. Pembaruan fitur keamanan umum.	
v1.16.0	v1.16.0	Rilis awal agen GuardDuty keamanan untuk instans Amazon ECS-EC2 Bottlerocket. Mendukung Bottlerocket ECS-2 dan ECS-3 varian (x86_64 dan aarch64).	Juli 17, 2026

GuardDuty versi agen keamanan untuk AWS Fargate (Hanya Amazon ECS)

Tabel berikut menunjukkan riwayat versi rilis untuk agen GuardDuty keamanan untuk Fargate (hanya Amazon ECS).

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
v1.17.1	x86_64 (AMD64): `sha256:27b27c489113ae83a272b5c98112e043f66faf`	Menambahkan dukungan untuk Kernel 7.2. Saat startup, agen mendeteksi jenis GuardDuty konektivi	September 09, 2026

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
	8379838bb 38e2d815d d6dfbf3a Graviton (ARM64): sha256:19 5078e4850 5cb05b06e 61df255fc 85a6d7917 b28678956 c75b11e69 855bdff3	tas dan mencoba terhubung ke titik akhir guardduty-data-v2 melalui link-local. Pembaruan fitur keamanan umum.	
v1.16.0	x86_64 (AMD64): sha256:71 1fa37e2cc e0417ba33 10d81439d 6b11170e4 46f685146 b36916e4e 38c1560d Graviton (ARM64): sha256:68 51e00893e ee958085a daccddf91 bdc009ebd dcd46b4da 6fb1962b1 32d47454	Pembaruan fitur keamanan umum.	Juli 17, 2026

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.15.0	x86_64 (AMD64):
	`sha256:66446df341bee1a1e218aa46b7807d0d0470266c8f374c5dbd97efcdb8356348`
	
	Graviton (ARM64):
	`sha256:b0def2aa8cab6b2060c703f386fdb29dc4166054e0509a9362b21a6ed7f9def7`
		Kemampuan agen baru untuk mendukung pengumpulan peristiwa yang dioptimalkan, memungkinkan penyebaran filter yang lebih cepat dan kecepatan deteksi yang lebih baik.
		
		Pembaruan fitur keamanan umum.
			28 Mei 2026

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.9.0	x86_64 (AMD64):
	`sha256:fd9acaa2326f180f0ed0c5a25d8ff0a2d0498a6e900c34c68d4e973ea7fb26a8`
	
	Graviton (ARM64):
	`sha256:0b04f8c28956684e752677bfd83dbc45afc8a43f7791fa44667b8078ba48a295`
		Penyetelan kinerja umum dan peningkatan keamanan.	Oktober 28, 2025

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.8.0	x86_64 (AMD64):
	`sha256:44 25417f39e 38b24c1be 428bacad1 dad53e064 5530dcf44 22436353b fe358e3a`
	
	Graviton (ARM64):
	`sha256:af f069418fd 6825846f8 f575c4990 6a67c8a44 6d12d9ed0 d21ab95bd 0d05497b`
		Penyetelan dan peningkatan kinerja umum.	Agustus 12, 2025

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.7.0	x86_64 (AMD64):
	`sha256:bf9197abdf853607e5fa392b4f97ccdd6ca56dd179be3ce8849e552d96582ac8`
	
	Graviton (ARM64):
	`sha256:56c8683c948bcd82c0dbcebf755204365ac7285994693c11717bd45f86e279c2`
		Resolusi ID kontainer yang ditingkatkan.
		
		Penyetelan dan peningkatan kinerja umum.
			April 04, 2025

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.6.0	x86_64 (AMD64):
	`sha256:c8dea71d372bc47b2f236f7a091b9a9b06bc8193c1cfe4c9346eb50f89258897`
	
	Graviton (ARM64):
	`sha256:f4032a566b90537646c2a987bef42eca1b498078ccc58a848603f877971a8dbe`
		Penyetelan dan peningkatan kinerja umum.	Februari 6, 2025

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.5.0	x86_64 (AMD64):
	`sha256:5e6fdc41f9eb748219d0498cd6c1dba6a19d875daec50167a0ac80e5028eac54`
	
	Graviton (ARM64):
	`sha256:d56801ff6864d601474010103b70b1c38431851358d182613bede20fe21090e734`
		Support untuk tugas ARM untuk `.../MetadataDNSRebind` temuan.
		
		Penyetelan dan peningkatan kinerja umum.
			November 14, 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.4.1	x86_64 (AMD64):
	`sha256:ef36a11151ec2d3d7db22273bfb954750dee76f0ac7bec37a7ba7e74c3de1c78`
	
	Graviton (ARM64):
	`sha256:a8844544a59d6b4cba98f8e528b513ac2d97432f208e3ad497cc16b331aa9faa`
		Pengerasan gambar kontainer.
		
		Penyetelan dan peningkatan kinerja umum.
			Oktober 24, 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.3.1	x86_64 (AMD64):
	`sha256:a6e2307d796e2875907bc4c1c69622c906f3192ddc42ef27b99e0a8f0979f3e0`
	
	Graviton (ARM64):
	`sha256:ad1b6539d806edb504f17e6bcfb8b4026c5e822300afc31c0d23c6a08f9b99e9`
		Support untuk resolver DNS kustom.	September 11, 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.3.0	x86_64 (AMD64):
	`sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831`
	
	Graviton (ARM64):
	`sha256:ff81a755d46681e409f55a95beedae9ebbcf5336e1c0b1e6348af7c6518bdbb1`
		Penyetelan dan peningkatan kinerja umum.
		
		Termasuk dukungan untuk menangkap sinyal keamanan tambahan untuk masa depan GuardDuty [GuardDuty Jenis penemuan Runtime Monitoring]().
			Agustus 9, 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
v1.2.0	x86_64 (AMD64): sha256:1d bad20ac2d c66d52d00 bb28dde42 81fe0d3c5 f261b1649 b247c2369 d9e26b93 Graviton (ARM64): sha256:91 930f8446f 5f95b93b8 ccb187739 92affa401 eb3f42da8 9d68077a5 6bafa6cd	Penyetelan dan peningkatan kinerja umum.	31 Mei 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.1.0	x86_64 (AMD64):
	`sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c9f673f2835823957e9dcf71657`
	
	Graviton (ARM64):
	`sha256:0d4b61648d7bdeab8ab8d94684f805498927c7d437d318204dcccfe8c9383dc7`
		Mendukung sinyal dan temuan keamanan baru.
		
		Penyetelan dan peningkatan kinerja umum.
			01 Mei 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.0.1	x86_64 (AMD64):
	`sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68`
	
	Graviton (ARM64):
	`sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7`
		Penyetelan dan peningkatan kinerja umum.	Januari 26, 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan

v1.0.0	x86_64 (AMD64):
	`sha256:35 9b8b014e5 076c625da a1056090e 522631587 a7afa3b2e 055edda6b d1141017`
	
	Graviton (ARM64):
	`sha256:b9 438690fa8 a86067180 a11658bec 0f4f838ae 3fbd225d0 4b9306250 648b3984`
		Rilis awal agen GuardDuty keamanan untuk AWS Fargate (hanya Amazon ECS).	26 November 2023

GuardDuty versi agen keamanan untuk sumber daya Amazon EKS

GuardDuty merilis versi agen yang diperbarui dari waktu ke waktu. Ketika GuardDuty mengelola agen secara otomatis, itu dirancang untuk mengelola pembaruan agen atas nama Anda. Saat Anda mengelola agen secara manual, Anda bertanggung jawab untuk memperbarui versi agen untuk kluster Amazon EKS Anda.

Sebelum memperbarui agen ke versi tertentu, tambahkan registri gambar GuardDuty ke `allowed-container-registries` dalam pengontrol penerimaan Anda. Untuk informasi selengkapnya, lihat Agen hosting repositori Amazon ECR GuardDuty.

Tabel berikut menunjukkan riwayat versi rilis GuardDuty agen add-on Amazon EKS.

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.17.1	x86_64 (AMD64): `sha256:8d772f754e9af50a63ab6af74ea24c12a5a3fb8a803c7cbc35ffaca3746c0540` Graviton (ARM64): `sha256:e5531367e9ffa539e409e99bbf49e804f01fdd894ee9322858b9bca703cd4016`	Menambahkan dukungan untuk Kernel 6.19, 7.0, 7.1. Saat startup, agen mendeteksi jenis GuardDuty konektivitas dan mencoba terhubung ke titik akhir guardduty-data-v2 melalui link-local. Pembaruan fitur keamanan umum.	September 09, 2026	–
v1.16.0	x86_64 (AMD64): `sha256:8a4ef4b5b5e6fce0a4b5a13922e65179293ee15a8812a2c7678b1c4b31e1f305`	Menambahkan dukungan untuk Kernel 6.19, 7.0, 7.1. Pembaruan fitur keamanan umum.	Juli 17, 2026	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
	Graviton (ARM64): `sha256:0a73c1d905a39db94f6ea37d98784dac84961e9199935fae20345de7aa3a57b7`			
v1.15.0	x86_64 (AMD64): `sha256:512642a5f9d9a316aa9100368acfdbae2481be7a5cfe9929571c1bb6e19c66fe` Graviton (ARM64): `sha256:f017e755615ae999fe5f163886f681508e8f53feea7e64e7ada733cdedb368d8`	Kemampuan agen baru untuk mendukung pengumpulan peristiwa yang dioptimalkan, memungkinkan penyebaran filter yang lebih cepat dan kecepatan deteksi yang lebih baik. Pembaruan fitur keamanan umum.	14 Mei 2026	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.12.2	x86_64 (AMD64): `sha256:06c25ab9fff7ee93048e5f34148c9627366323 5937199b4bd2e28b5ee2e5c080` Graviton (ARM64): `sha256:f89962d971350ff6ab408cf6ec7bca9dd06152 f0172b7f9c68ae770cc0fc4598`	Pembaruan fitur keamanan umum.	Maret 26, 2026	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.12.1	x86_64 (AMD64): `sha256:f29a597745e5acff48809bebac7d8091bbc38229453dd26710c549b817362491` Graviton (ARM64): `sha256:089cebdc7e891177e107a099c9a4e362d9d74b5362cd374b448a16078040f6c6`	Penyetelan kinerja umum dan pembaruan fitur keamanan.	Nov 17, 2025	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.11.0	x86_64 (AMD64): `sha256:7c398fd50dee5fe493c361aa7fe191e094ddfa000c65b449a9ed6a5cd53610e7` Graviton (ARM64): `sha256:98a547b47d4770f45e75eb9730c807d9265722ca2f391e0aa5cb19e487ab455f`	Menambahkan dukungan untuk distribusi Fedora 40 dan Fedora 41 OS. Untuk informasi lebih lanjut, lihat Memvalidasi persyaratan arsitektur (untuk EKS). Penyetelan kinerja umum dan peningkatan keamanan.	Agustus 29, 2025	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.10.0	x86_64 (AMD64): `sha256:6dcbe5b055e1ef0af903071ede0b08f755ad5b7e9774a67df5399efdaa1f3d7d` Graviton (ARM64): `sha256:f0536882268 9610a4bab543abf93d3e070b1b559e62a2e67d82dfa9837600f72`	Resolusi ID kontainer yang ditingkatkan. Penyetelan dan peningkatan kinerja umum.	April 04, 2025	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.9.0	x86_64 (AMD64): `sha256:51c5789ef6570f9bec879ac48a8f4769718cbc31e45430032569917e219af63f` Graviton (ARM64): `sha256:9c2f74e7ea0827b7e422ae4c91fffc6c2bc41a1cdb96c7191d05259d337154e1`	Penyetelan dan peningkatan kinerja umum.	Maret 02, 2025	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.8.1	x86_64 (AMD64): `sha256:f2ce8cf89dbe17e3388cecb35053544dadf21af7770545f8d4b50384076aff47` Graviton (ARM64): `sha256:30f586e4b694e704bcafadfa9081ab0aeff3cfbcde39743a0f1e24f77d79627f`	Menambahkan dukungan untuk CentOS Stream 9.0, RedHat 9.4, Fedora 34.0, dan Ubuntu 24.04. Support untuk instance ARM untuk `.../MetadataDNSRebind` menemukan. Penyetelan dan peningkatan kinerja umum.	November 23, 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.7.1	x86_64 (AMD64): `sha256:b8b86b5d0872c8b67fecf64ec3d17266636054` `5435a1752447d510951a7fd749` Graviton (ARM64): `sha256:40ac4cfc354fd430ba7897ca1632e9a500ed13eeb0c315c5bcad38680e76b6e9`	Penyetelan dan peningkatan kinerja umum. Termasuk dukungan untuk menangkap sinyal keamanan tambahan untuk masa depanGuardDuty Jenis penemuan Runtime Monitoring. Support untuk resolver DNS kustom.	September 13, 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.7.0	x86_64 (AMD64): `sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffcd7e68554a423d610cea8c7e8f2185ec` Graviton (ARM64): `sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbe47ecfaeb2784435cf67ebe0a`	Penyetelan dan peningkatan kinerja umum. Termasuk dukungan untuk menangkap sinyal keamanan tambahan untuk masa depanGuardDuty Jenis penemuan Runtime Monitoring.	Agustus 17, 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.6.1	x86_64 (AMD64): `sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bdb07c3ab1` Graviton (ARM64): `sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019`	Penyetelan dan peningkatan kinerja umum.	14 Mei 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.6.0	x86_64 (AMD64): `sha256:7dabcbee30d8b053676752fbc19e89f77272d9a6a53cc93731f5872180ef9010` Graviton (ARM64): `sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650`	• Mendukung konfigurasi agen GuardDuty otomatis untuk EKS/EC2 sumber daya. • Mendukung sinyal dan temuan keamanan baru. Untuk informasi selengkapnya, lihat Jenis acara runtime yang dikumpulkan yang menggunakan GuardDuty dan GuardDuty Jenis penemuan Runtime Monitoring. • Penyetelan dan peningkatan kinerja umum.	April 29, 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.5.0	x86_64 (AMD64): `sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d` Graviton (ARM64): `sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6`	• Penyetelan dan peningkatan kinerja umum. • Peningkatan keamanan termasuk jenis acara baru di bawah. Jenis acara runtime yang dikumpulkan • Peningkatan kinerja seputar penggunaan CPU.	07 Maret 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.4.1	x86_64 (AMD64): `sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c` Graviton (ARM64): `sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40`	Penyetelan dan peningkatan kinerja umum.	Januari 16, 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.4.0	x86_64 (AMD64): `sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f` Graviton (ARM64): `sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e`	Manifest mount point mendukung pengumpulan data yang lebih baik AppArmor konfigurasi dalam manifes Kumpulkan argumen baris perintah Penyetelan dan penyempurnaan kinerja umum	21 Desember 2023	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.3.1	x86_64 (AMD64): `sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29` Graviton (ARM64): `sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd`	Patch dan pembaruan keamanan penting.	23 Oktober 2023	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.3.0	x86_64 (AMD64): `sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694` Graviton (ARM64): `sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb`	Mendukung platform Ubuntu Mendukung Kubernetes versi 1.28 Peningkatan kinerja umum dan peningkatan stabilitas.	Oktober 05, 2023	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.2.0	x86_64 (AMD64): `sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3` Graviton (ARM64): `sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa`	Selain AMD64-based instance, v1.2.0 sekarang juga mendukung ARM64-based instance. Menambahkan dan memverifikasi dukungan untuk Bottlerocket Mendukung Kubernetes versi 1.27 Peningkatan kinerja umum dan peningkatan stabilitas.	Juni 16, 2023	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar [1]
v1.1.0	`sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c`	Selain ituVersi Kubernetes didukung oleh agen keamanan GuardDuty, rilis agen ini juga mendukung Kubernetes versi 1.26. Peningkatan kinerja umum dan peningkatan stabilitas.	2 Mei 2023	14 Mei 2024
v1.0.0	`sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e`	Rilis awal agen add-on Amazon EKS.	30 Maret 2023	14 Mei 2024

[1] Untuk informasi tentang memperbarui versi agen Anda saat ini yang mendekati akhir dukungan standar, lihatMemperbarui agen keamanan secara manual untuk sumber daya Amazon EKS.

Sumber daya tambahan - langkah selanjutnya

Untuk informasi selengkapnya tentang langkah selanjutnya, lihat topik berikut:

- Prasyarat untuk mengaktifkan Pemantauan Runtime- Dengan versi agen baru, mungkin ada pembaruan ke bagian prasyarat. Verifikasi dan validasi bahwa sumber daya Anda memenuhi prasyarat terbaru.
- Mengelola agen GuardDuty keamanan- Ketika Anda mengelola agen secara manual, maka Anda bertanggung jawab untuk mengelola pembaruan ke versi agen yang berjalan pada sumber daya Anda. Berdasarkan jenis sumber daya Anda (Amazon EC2-Amazon EKS atau Amazon ECS), lakukan langkah-langkah untuk memperbarui agen keamanan. Pastikan juga untuk memvalidasi konfigurasi titik akhir VPC Anda.
- Meninjau statistik cakupan runtime dan masalah pemecahan masalah- Setelah Anda memperbarui agen keamanan, Anda dapat menilai cakupan runtime sumber daya Anda. Jika ada masalah cakupan, gunakan langkah pemecahan masalah terkait.

Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring

Bagian ini berlaku untuk Anda Akun AWS jika Anda memilih untuk menonaktifkan Runtime Monitoring, atau hanya konfigurasi agen GuardDuty otomatis untuk jenis sumber daya.

Menonaktifkan konfigurasi agen GuardDuty otomatis

GuardDuty tidak menghapus agen keamanan yang digunakan pada sumber daya Anda. Namun, GuardDuty akan berhenti mengelola pembaruan ke agen keamanan.

GuardDuty terus menerima peristiwa runtime dari jenis sumber daya Anda. Untuk mencegah dampak pada statistik penggunaan Anda, pastikan untuk menghapus agen GuardDuty keamanan dari sumber daya Anda.

Apakah Akun AWS menggunakan titik akhir VPC bersama atau tidak, GuardDuty tidak menghapus titik akhir VPC. Jika diperlukan, Anda harus menghapus titik akhir VPC secara manual.

Menonaktifkan Runtime Monitoring dan EKS Runtime Monitoring

Bagian ini berlaku untuk Anda dalam skenario berikut:

- Anda tidak pernah mengaktifkan EKS Runtime Monitoring secara terpisah dan sekarang Anda menonaktifkan Runtime Monitoring.

- Anda menonaktifkan Runtime Monitoring dan EKS Runtime Monitoring. Jika Anda tidak yakin tentang status konfigurasi EKS Runtime Monitoring, lihat. Memeriksa status konfigurasi EKS Runtime Monitoring

  > **Menonaktifkan Runtime Monitoring tanpa menonaktifkan EKS Runtime Monitoring**
  >
  > Dalam skenario ini, di beberapa titik waktu, Anda mengaktifkan EKS Runtime Monitoring, dan kemudian, juga mengaktifkan Runtime Monitoring tanpa menonaktifkan EKS Runtime Monitoring.
  > Sekarang, ketika Anda menonaktifkan Runtime Monitoring, Anda juga perlu menonaktifkan EKS Runtime Monitoring; jika tidak, Anda akan terus mengeluarkan biaya penggunaan untuk EKS Runtime Monitoring.

Jika skenario yang tercantum sebelumnya berlaku untuk Anda, maka GuardDuty akan mengambil tindakan berikut di akun Anda:

- GuardDuty menghapus titik akhir VPC yang memiliki `GuardDutyManaged` tag:. `true` Ini adalah VPC yang GuardDuty telah dibuat untuk mengelola agen keamanan otomatis.
- GuardDuty menghapus grup keamanan yang ditandai sebagai`GuardDutyManaged`:. `true`
- Untuk VPC bersama yang telah digunakan oleh setidaknya satu akun peserta, GuardDuty tidak menghapus titik akhir VPC maupun grup keamanan yang terkait dengan sumber daya VPC bersama.
- Untuk sumber daya Amazon GuardDuty EKS, hapus agen keamanan. Ini independen dari apakah itu dikelola secara manual atau melalui GuardDuty.

  Untuk sumber daya Amazon ECS, karena tugas ECS tidak dapat diubah, tidak GuardDuty dapat menghapus instalan agen keamanan dari sumber daya tersebut. Ini tidak tergantung pada bagaimana Anda mengelola agen keamanan — secara manual atau otomatis melalui GuardDuty. Setelah Anda menonaktifkan Runtime Monitoring, tidak GuardDuty akan melampirkan wadah sespan saat tugas ECS baru mulai berjalan. Untuk informasi tentang bekerja dengan Fargate-ECS tugas, lihatMenyebarkan agen keamanan ke Amazon ECS di Fargate.

  Untuk sumber daya Amazon EC2, GuardDuty hapus instalan agen keamanan dari semua instans Amazon EC2 yang dikelola Systems Manager (SSM) hanya jika memenuhi ketentuan berikut:

  - Sumber daya Anda tidak ditandai dengan`GuardDutyManaged`: tag `false` pengecualian.

- GuardDuty harus memiliki izin untuk mengakses tag dalam metadata instance. Untuk sumber daya EC2 ini, Access to tag dalam metadata instance disetel ke Allow.

Ketika Anda berhenti mengelola agen keamanan secara manual

Terlepas dari pendekatan mana yang Anda gunakan untuk menyebarkan dan mengelola agen GuardDuty keamanan, untuk berhenti memantau peristiwa runtime di sumber daya Anda, Anda harus menghapus agen GuardDuty keamanan. Jika Anda ingin berhenti memantau peristiwa runtime dari jenis sumber daya di akun, Anda juga dapat menghapus titik akhir Amazon VPC.

Menghapus instalan agen keamanan secara manual untuk sumber daya Amazon EC2

Bagian ini menyediakan metode untuk menghapus instalan agen GuardDuty keamanan dari sumber daya Amazon EC2 Anda. Ketika Anda mengelola agen keamanan secara manual, Anda bertanggung jawab untuk menghapus agen dari sumber daya. GuardDuty tidak mengambil tindakan apa pun pada sumber daya yang Anda kelola.

Jika Anda membuat titik akhir VPC Amazon secara manual, maka setelah Anda menghapus instalan agen keamanan pada semua jenis sumber daya yang dipantau di akun Anda, Anda dapat memilih untuk menghapus titik akhir VPC. Ini adalah langkah terpisah. Untuk informasi selengkapnya, lihat To delete a VPC endpoint.

Berdasarkan cara Anda menginstal agen keamanan di sumber daya Anda, pilih salah satu metode berikut untuk menghapusnya.

Topik

- Metode 1 - Dengan menggunakan perintah Run
- Metode 2 - Dengan menggunakan Linux Package Managers

Metode 1 - Dengan menggunakan perintah Run

Saat Anda menginstal agen keamananMetode 1 - Menggunakan AWS Systems Manager, lakukan langkah-langkah berikut untuk menghapus instalan agen:

Untuk menghapus instalan agen GuardDuty keamanan

1. Anda dapat menghapus instalan agen GuardDuty keamanan dengan mengikuti langkah-langkah seperti yang ditentukan dalam AWS Systems Manager Jalankan Perintah di Panduan AWS

Systems Manager Pengguna. Gunakan tindakan Uninstall dalam parameter untuk menghapus instalan agen GuardDuty keamanan.

Di bagian Target, pastikan dampaknya hanya pada instans Amazon EC2 yang ingin Anda hapus instalan agen keamanan.

Gunakan GuardDuty dokumen dan distributor berikut:

- Nama dokumen: `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`
- Distributor: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`

2. Setelah memberikan semua detail, saat Anda memilih Jalankan, agen keamanan yang disebarkan pada instans Amazon EC2 yang ditargetkan akan dihapus.

   Untuk menghapus konfigurasi endpoint Amazon VPC, Anda harus menonaktifkan Runtime Monitoring dan Amazon EKS Runtime Monitoring.

3. Jika Anda juga ingin menghapus titik akhir VPC yang terkait dengan agen keamanan ini, lihat. To delete a VPC endpoint

Metode 2 - Dengan menggunakan Linux Package Managers

Saat Anda menginstal agen keamananMetode 2 - Menggunakan Linux Package Manager, lakukan langkah-langkah berikut untuk menghapus instalan agen:

Untuk menghapus instalan agen GuardDuty keamanan

1. Terhubung ke instans Anda. Untuk langkah-langkah tentang cara melakukannya, lihat Connect ke instans Linux menggunakan klien SSH di Panduan Pengguna Amazon EC2.
2. Perintah untuk menghapus instalasi

   Perintah berikut akan menghapus instalan agen GuardDuty keamanan dari instans Amazon EC2 yang Anda sambungkan:

   - Untuk RPM:

     ```
     sudo rpm -e amazon-guardduty-agent
     ```

   - Untuk Debian:

```
sudo dpkg --purge amazon-guardduty-agent
```

Setelah Anda menjalankan perintah, Anda juga dapat memeriksa log yang terkait dengan perintah.

3. Jika Anda juga ingin menghapus titik akhir VPC yang terkait dengan agen keamanan ini, lihat. To delete a VPC endpoint

Menghapus instalan agen keamanan untuk sumber daya ECS-EC2 Bottlerocket

Lakukan langkah-langkah berikut untuk menghapus instalan agen GuardDuty keamanan dari instance Bottlerocket ECS-EC2 Anda.

Untuk menghapus instalan agen GuardDuty keamanan

1. Untuk menghapus instalan agen GuardDuty keamanan, gunakan AWS Systems Manager Run Command (di Panduan AWS Systems Manager Pengguna) dan atur parameter tindakan ke Uninstall.

   Di bagian Target, pastikan bahwa dampaknya hanya pada instance Bottlerocket yang ingin Anda hapus instalan agen keamanan.

   Gunakan GuardDuty dokumen dan distributor berikut:

   - Nama dokumen:`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
   - Distributor:`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`.
2. Setelah Anda memberikan semua detail dan memilih Jalankan, GuardDuty hapus agen keamanan dari instance Bottlerocket yang ditargetkan.
3. Untuk juga menghapus titik akhir VPC yang terkait dengan agen keamanan ini, lihat. To delete a VPC endpoint

Membersihkan sumber daya agen keamanan

Bagian ini menjelaskan bagaimana Anda dapat membersihkan AWS sumber daya yang terkait dengan agen keamanan. Seperti yang tercantum dalamMenonaktifkan, menghapus instalasi, dan

pembersihan sumber daya, tidak GuardDuty akan menghapus atau menghapus semua sumber daya agen keamanan. Bagian berikut memberikan petunjuk tentang bagaimana Anda dapat menghapus sumber daya agen keamanan.

Untuk menghapus titik akhir Amazon VPC

Saat Anda mengelola agen keamanan secara manual, Anda mungkin telah membuat titik akhir VPC Amazon secara manual. Setelah menghapus instalan agen keamanan untuk semua sumber daya yang dipantau di akun Anda, Anda dapat memilih untuk menghapus titik akhir VPC ini.

Daftar berikut menyediakan skenario saat menggunakan VPC bersama dibandingkan dengan tidak menggunakan VPC bersama.

- Tanpa VPC bersama — Saat Anda tidak lagi ingin memantau sumber daya di akun, pertimbangkan untuk menghapus titik akhir VPC Amazon.
- Dengan VPC bersama — Saat akun pemilik VPC bersama menghapus sumber daya VPC bersama yang masih digunakan, status cakupan Runtime Monitoring (dan bila berlaku, EKS Runtime Monitoring) untuk sumber daya di akun pemilik VPC bersama Anda dan akun yang berpartisipasi mungkin menjadi tidak sehat. Untuk informasi tentang status cakupan, lihatMeninjau statistik cakupan runtime dan masalah pemecahan masalah.

Untuk menghapus titik akhir VPC, lihat Menghapus titik akhir antarmuka di Panduan.AWS PrivateLink

Untuk menghapus grup keamanan

- Tanpa VPC bersama - Jika Anda tidak lagi ingin memantau jenis sumber daya di akun, pertimbangkan untuk menghapus grup keamanan yang terkait dengan VPC Amazon.
- Dengan VPC bersama — Saat akun pemilik VPC bersama menghapus grup keamanan, akun peserta apa pun yang saat ini menggunakan grup keamanan yang terkait dengan VPC bersama, status cakupan Pemantauan Waktu Proses untuk sumber daya di akun pemilik VPC bersama Anda dan akun yang berpartisipasi mungkin menjadi tidak sehat. Untuk informasi selengkapnya, lihat Meninjau statistik cakupan runtime dan masalah pemecahan masalah.

Untuk selengkapnya tentang langkah-langkah, lihat Menghapus grup keamanan Amazon EC2 di Panduan Pengguna Amazon EC2.

Untuk menghapus agen GuardDuty keamanan dari cluster EKS

Untuk menghapus agen keamanan dari kluster EKS yang tidak ingin Anda pantau lagi, lihat Menghapus add-on Amazon EKS dari klaster di Panduan Pengguna Amazon EKS.

Menghapus agen add-on EKS tidak menghapus `amazon-guardduty` namespace dari kluster EKS. Untuk menghapus `amazon-guardduty` namespace, lihat Menghapus namespace.

Untuk menghapus **`amazon-guardduty`** namespace (kluster EKS)

Menonaktifkan konfigurasi agen otomatis tidak secara otomatis menghapus `amazon-guardduty` namespace dari kluster EKS Anda. Untuk menghapus `amazon-guardduty` namespace, lihat Menghapus namespace.

GuardDuty Perlindungan Malware untuk EC2

Perlindungan Malware untuk EC2 membantu Anda mendeteksi potensi keberadaan malware dengan memindai volume Amazon Elastic Block Store (Amazon EBS) yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) dan beban kerja container yang berjalan di Amazon EC2. Perlindungan Malware untuk EC2 menyediakan opsi pemindaian di mana Anda dapat memutuskan apakah Anda ingin menyertakan atau mengecualikan instans Amazon EC2 tertentu pada saat pemindaian. Ini juga menyediakan opsi untuk menyimpan snapshot volume Amazon EBS yang dilampirkan ke instans Amazon EC2 atau beban kerja kontainer, di akun Anda. GuardDuty Snapshot dipertahankan hanya ketika malware ditemukan dan Perlindungan Malware untuk temuan EC2 dihasilkan.

Perlindungan Malware untuk EC2 dirancang sedemikian rupa sehingga tidak akan memengaruhi kinerja sumber daya Anda. Untuk informasi tentang cara kerja Perlindungan Malware untuk EC2 GuardDuty, lihatCara GuardDuty memindai volume EBS untuk deteksi malware. Untuk informasi tentang ketersediaan Perlindungan Malware untuk EC2 yang berbeda Wilayah AWS, lihatWilayah dan titik akhir.

> **Catatan**
>
> Perlindungan Malware untuk EC2 mendukung pemindaian malware pada instans terkelola untuk Mode Otomatis Amazon EKS. Untuk selengkapnya lihat dukungan Instans Terkelola di Guardduty.
> Perlindungan Malware untuk EC2 tidak mendukung pemindaian malware untuk AWS Fargate beban kerja yang berjalan dengan Amazon EKS atau Amazon ECS.
> Untuk informasi tentang fitur Amazon EKS ini, lihat Apa itu Amazon EKS? di Panduan Pengguna Amazon EKS.

Topik

- Membandingkan pemindaian GuardDuty-initiated malware dan pemindaian On-demand malware
- Cara GuardDuty memindai volume EBS untuk deteksi malware
- Volume Amazon EBS yang didukung untuk pemindaian malware
- Mengatur retensi snapshot dan cakupan pemindaian EC2
- GuardDuty-initiated pemindaian malware
- On-demand pemindaian malware GuardDuty

- Memantau status pemindaian dan hasil dalam Perlindungan Malware untuk EC2
- GuardDuty akun layanan oleh Wilayah AWS
- Kuota dalam Perlindungan Malware untuk EC2

Membandingkan pemindaian GuardDuty-initiated malware dan pemindaian On-demand malware

Perlindungan Malware untuk EC2 menawarkan dua jenis pemindaian untuk mendeteksi aktivitas yang berpotensi berbahaya di instans Amazon EC2 dan beban kerja kontainer Anda GuardDuty-initiated — pemindaian malware dan pemindaian malware. On-demand Tabel berikut menunjukkan perbandingan antara kedua jenis pemindaian.

Faktor	GuardDuty-initiated pemindaian malware	On-demand pemindaian malware
Bagaimana pemindaian dipanggil	Setelah Anda mengaktifkan pemindaian GuardDuty-initiated malware, setiap kali GuardDuty menghasilkan temuan yang menunjukkan potensi keberadaan malware dalam instans Amazon EC2 atau beban kerja kontainer, GuardDuty secara otomatis memulai pemindaian malware tanpa agen pada volume Amazon EBS yang dilampirkan ke sumber daya Anda yang berpotensi terkena dampak. Untuk informasi selengkapnya, lihat GuardDuty-initiated pemindaian malware.	Anda dapat memulai pemindaian On-demand malware dengan memberikan Nama Sumber Daya Amazon (ARN) instans Amazon EC2 Anda. Anda dapat memulai pemindaian On-demand malware bahkan ketika tidak ada GuardDuty temuan yang dihasilkan untuk sumber daya Anda. Untuk informasi selengkapnya, lihat On-demand pemindaian malware GuardDuty.
Konfigurasi diperlukan	Untuk menggunakan pemindaian GuardDuty-initiated malware, Anda	Akun Anda harus GuardDuty diaktifkan. Untuk menggunakan pemindaian On-demand

Faktor	GuardDuty-initiated pemindaian malware	On-demand pemindaian malware
	harus mengaktifkannya untuk akun Anda. Untuk mengelola beberapa akun dengan menggunakan AWS Organizations atau metode berbasis undangan, lihatMengaktifkan pemindaian GuardDuty-initiated malware di lingkungan beberapa akun. Untuk mengaktifkan pemindaian GuardDuty-initiated malware di akun Anda sendiri, lihatMengaktifkan pemindaian GuardDuty-initiated malware untuk akun mandiri.	malware, tidak ada konfigurasi yang diperlukan di tingkat fitur.
Tunggu waktu untuk memulai pemindaian baru	Setiap kali GuardDuty menghasilkan salah satuTemuan yang memanggil pemindaian GuardDuty-initiated malware, pemindaian malware dimulai secara otomatis hanya sekali setiap 24 jam.	Anda dapat memulai pemindaian On-demand malware pada sumber daya yang sama kapan saja setelah 1 jam dari waktu mulai pemindaian sebelumnya.

Faktor	GuardDuty-initiated pemindaian malware	On-demand pemindaian malware
Ketersediaan periode uji coba gratis 30 hari [1]	Saat Anda mengaktifkan pemindaian GuardDuty-initiated malware untuk pertama kalinya di akun Anda, Anda dapat menggunakan periode uji coba gratis 30 hari. Untuk informasi selengkapnya, lihat Uji coba gratis 30 hari dalam pemindaian GuardDuty-initiated malware.	Tidak ada periode uji coba gratis dengan pemindaian On-demand malware untuk GuardDuty akun baru atau yang sudah ada.
Opsi pemindaian [2]	Setelah mengonfigurasi pemindaian GuardDuty-initiated malware, Perlindungan Malware untuk EC2 menyediakan opsi untuk memindai atau melewati sumber daya Amazon EC2 tertentu dengan menggunakan tag. Perlindungan Malware untuk EC2 tidak akan memulai pemindaian otomatis pada sumber daya yang Anda pilih untuk dikecualikan dari pemindaian. Untuk informasi selengkapnya, lihat Opsi pindai dengan tag yang ditentukan pengguna.	Karena Anda menyediakan sumber daya ARN untuk memulai pemindaian malware sesuai permintaan secara manual, penggunaan Opsi pindai dengan tag yang ditentukan pengguna tidak berlaku.

[1] Anda akan dikenakan biaya penggunaan untuk membuat snapshot volume EBS dan mempertahankan snapshot. Untuk informasi selengkapnya tentang mengonfigurasi akun Anda untuk menyimpan snapshot, lihat. Retensi snapshot

[2] Baik pemindaian GuardDuty-initiated On-demand malware dan pemindaian malware mendukung menggunakan tag global untuk mengecualikan sumber daya Amazon EC2 dari pemindaian malware. Untuk informasi selengkapnya, lihat `GuardDutyExcludedTag` global.

Cara GuardDuty memindai volume EBS untuk deteksi malware

Bagian ini menjelaskan cara Perlindungan Malware untuk EC2, termasuk pemindaian GuardDuty-initiated malware dan pemindaian On-demand malware, memindai volume Amazon EBS yang terkait dengan instans Amazon EC2 dan beban kerja kontainer Anda. Sebelum melanjutkan, pertimbangkan penyesuaian berikut:

- Opsi pemindaian — Perlindungan Malware untuk EC2 menawarkan kemampuan untuk menentukan tag untuk menyertakan atau mengecualikan instans Amazon EC2 dan volume Amazon EBS dari proses pemindaian. Hanya pemindaian GuardDuty-initiated malware yang mendukung opsi pemindaian dengan tag yang ditentukan pengguna. Pemindaian GuardDuty-initiated On-demand malware dan pemindaian malware mendukung `GuardDutyExcluded` tag global. Untuk informasi selengkapnya, lihat Opsi pindai dengan tag yang ditentukan pengguna.
- Retensi snapshot — Perlindungan Malware untuk EC2 menyediakan opsi untuk menyimpan snapshot volume Amazon EBS Anda di akun Anda. AWS Secara default, pengaturan ini dimatikan. Anda dapat memilih penyimpanan snapshot untuk pemindaian malware GuardDuty yang dimulai dan sesuai permintaan. Untuk informasi selengkapnya, lihat Retensi snapshot.

Ketika GuardDuty menghasilkan satu atau lebihTemuan yang memanggil pemindaian GuardDuty-initiated malware, maka aktivitas ini akan menjadi alasan GuardDuty untuk memulai pemindaian malware. Jika opsi pemindaian Anda tidak mengecualikan instance ini, maka GuardDuty akan memulai pemindaian.

Untuk memulai pemindaian On-demand malware pada volume Amazon EBS yang terkait dengan instans Amazon EC2, berikan Nama Sumber Daya Amazon (ARN) instans Amazon EC2.

Sebagai tanggapan untuk memulai pemindaian malware sesuai permintaan atau pemindaian GuardDuty-initiated malware otomatis, GuardDuty buat snapshot dari volume EBS yang relevan yang melekat pada sumber daya yang berpotensi terkena dampak, dan membagikannya dengan. GuardDuty akun layanan Saat GuardDuty membuat snapshot volume EBS Anda, ia menambahkan tag default yang disebut. `GuardDutyScanId` Tag ini GuardDuty membantu mengakses snapshot. Pastikan Anda tidak menghapus tag ini. Dari snapshot ini, GuardDuty buat volume replika EBS terenkripsi di akun layanan.

Setelah pemindaian selesai, GuardDuty hapus volume EBS replika terenkripsi dan snapshot volume EBS Anda. Secara default, pengaturan retensi snapshot dimatikan. Namun, snapshot dipertahankan jika penguncian snapshot Amazon EBS diaktifkan untuk mereka, terlepas dari hasil dan pengaturan pemindaian. GuardDuty tidak dapat mengubah pengaturan kunci snapshot Amazon EBS.

Daftar berikut menjelaskan perilaku retensi snapshot, terlepas dari penguncian snapshot EBS:

Retensi snapshot diaktifkan:

- Ketika malware ditemukan, GuardDuty simpan snapshot di Anda. Akun AWS
- Ketika tidak ada malware yang ditemukan, GuardDuty tidak menyimpan snapshot kecuali terkunci.

Retensi snapshot dimatikan (pengaturan default):

- Apakah malware ditemukan atau tidak, snapshot tidak dipertahankan.
- GuardDuty tidak dapat menghapus snapshot Amazon EBS yang terkunci.

GuardDuty akan mempertahankan setiap replika volume EBS di akun layanan hingga 55 jam. Jika ada pemadaman layanan, atau kegagalan dengan volume EBS replika dan pemindaian malware, GuardDuty akan mempertahankan volume EBS tersebut selama tidak lebih dari tujuh hari. Periode retensi volume yang diperpanjang adalah untuk melakukan triase dan mengatasi pemadaman atau kegagalan. GuardDuty Perlindungan Malware untuk EC2 akan menghapus replika volume EBS dari akun layanan setelah pemadaman atau kegagalan ditangani, atau setelah periode retensi yang diperpanjang berakhir.

Untuk informasi tentang metodologi deteksi GuardDuty malware dan mesin pemindaian yang digunakannya, lihatGuardDuty mesin pemindai deteksi malware.

Volume Amazon EBS yang didukung untuk pemindaian malware

Di semua Wilayah AWS tempat GuardDuty mendukung fitur Perlindungan Malware untuk EC2, Anda dapat memindai volume Amazon EBS yang tidak terenkripsi atau dienkripsi. Anda dapat memiliki volume Amazon EBS yang dienkripsi dengan salah satu Kunci yang dikelola AWSatau kunci yang dikelola pelanggan. Saat ini, beberapa Wilayah di mana Perlindungan Malware untuk EC2 tersedia, dapat mendukung kedua cara untuk mengenkripsi volume Amazon EBS Anda, sementara yang lain hanya mendukung kunci yang dikelola pelanggan. Untuk informasi tentang Wilayah yang didukung, lihat danGuardDuty akun layanan oleh Wilayah AWS. Untuk informasi tentang Wilayah yang GuardDuty tersedia tetapi Perlindungan Malware untuk EC2 tidak tersedia, lihatRegion-specific ketersediaan fitur.

Daftar berikut menjelaskan kunci yang GuardDuty menggunakan apakah volume Amazon EBS Anda dienkripsi atau tidak:

- Volume Amazon EBS yang tidak dienkripsi atau dienkripsi Kunci yang dikelola AWS- GuardDuty menggunakan kuncinya sendiri untuk mengenkripsi replika volume Amazon EBS.

  Jika Wilayah Anda tidak mendukung pemindaian volume Amazon EBS yang dienkripsi dengan enkripsi Amazon EBS secara default, maka Anda perlu mengubah kunci default untuk menjadi kunci yang dikelola pelanggan. Ini akan membantu GuardDuty mengakses volume EBS ini. Dengan memodifikasi kunci, bahkan volume EBS future akan dibuat dengan kunci yang diperbarui sehingga GuardDuty dapat mendukung pemindaian malware. Untuk langkah-langkah untuk mengubah kunci default, lihat Ubah default AWS KMS ID kunci volume Amazon EBS di bagian berikutnya.
- Volume Amazon EBS yang dienkripsi dengan kunci yang dikelola pelanggan — GuardDuty menggunakan kunci yang sama untuk mengenkripsi volume replika EBS. Untuk informasi tentang kebijakan terkait AWS KMS enkripsi yang didukung, lihatService-linked izin peran untuk Perlindungan Malware untuk EC2.

Ubah default AWS KMS ID kunci volume Amazon EBS

Saat Anda menggunakan buat volume Amazon EBS dengan menggunakan enkripsi Amazon EBS, dan tidak menentukan ID AWS KMS kunci, volume Amazon EBS Anda akan dienkripsi dengan kunci default untuk enkripsi. Saat Anda mengaktifkan enkripsi secara default, Amazon EBS akan secara otomatis mengenkripsi volume dan snapshot baru dengan menggunakan kunci KMS default Anda untuk enkripsi Amazon EBS.

Anda dapat memodifikasi kunci enkripsi default dan menggunakan kunci yang dikelola pelanggan untuk enkripsi Amazon EBS. Ini akan membantu GuardDuty mengakses volume Amazon EBS ini. Untuk mengubah ID kunci default EBS, tambahkan izin yang diperlukan berikut ke kebijakan IAM Anda —. `ec2:modifyEbsDefaultKmsKeyId` Setiap volume Amazon EBS yang baru dibuat yang Anda pilih untuk dienkripsi tetapi tidak menentukan ID kunci KMS terkait, akan menggunakan ID kunci default. Gunakan salah satu metode berikut untuk memperbarui ID kunci default EBS:

Untuk mengubah ID kunci KMS default dari volume Amazon EBS

Lakukan salah satu tindakan berikut:

- Menggunakan API — Anda dapat menggunakan ModifyEbsDefaultKmsKeyIdAPI. Untuk informasi tentang cara melihat status enkripsi volume, lihat Membuat volume Amazon EBS.
- Menggunakan AWS CLI perintah - Contoh berikut memodifikasi ID kunci KMS default yang akan mengenkripsi volume Amazon EBS jika Anda tidak memberikan ID kunci KMS. Pastikan untuk mengganti Region dengan ID kunci KM Anda. Wilayah AWS

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
id AKIAIOSFODNN7EXAMPLE
```

Perintah di atas akan menghasilkan output yang mirip dengan output berikut:

```
{
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
}
```

Untuk informasi selengkapnya, lihat modify-ebs-default-kms-key-id.

Mengatur retensi snapshot dan cakupan pemindaian EC2

Bagian ini menjelaskan cara menyesuaikan opsi pemindaian malware untuk instans Amazon EC2 Anda. Kustomisasi ini berlaku untuk pemindaian On-demand malware dan yang diprakarsai oleh. GuardDuty Anda dapat melakukan tindakan berikut:

- Aktifkan retensi snapshot — Saat diaktifkan sebelum pemindaian, snapshot Amazon EBS GuardDuty akan tetap GuardDuty terdeteksi berbahaya.
- Pilih instans Amazon EC2 mana yang akan dipindai — Gunakan tag untuk menyertakan atau mengecualikan instans Amazon EC2 tertentu dari pemindaian malware.

Retensi snapshot

GuardDuty memberi Anda opsi untuk menyimpan snapshot volume EBS Anda di akun Anda AWS . Secara default, pengaturan retensi snapshot dimatikan. Snapshot hanya akan dipertahankan jika pengaturan ini diaktifkan sebelum pemindaian dimulai.

Saat pemindaian dimulai, GuardDuty hasilkan replika volume EBS berdasarkan snapshot volume EBS Anda. Setelah pemindaian selesai dan pengaturan retensi snapshot di akun Anda sudah diaktifkan, snapshot volume EBS Anda akan dipertahankan hanya ketika malware ditemukan dan

dihasilkan. Perlindungan Malware untuk jenis pencarian EC2 Jika tidak ada malware yang ditemukan, terlepas dari pengaturan snapshot Anda, GuardDuty secara otomatis menghapus snapshot volume EBS Anda kecuali penguncian snapshot Amazon EBS telah diaktifkan pada snapshot yang dibuat.

Biaya penggunaan snapshot

Selama pemindaian malware, seperti GuardDuty membuat snapshot volume Amazon EBS Anda, ada biaya penggunaan yang terkait dengan langkah ini. Jika Anda mengaktifkan pengaturan retensi snapshot untuk akun Anda, ketika malware ditemukan dan snapshot dipertahankan, Anda akan dikenakan biaya penggunaan untuk hal yang sama. Untuk informasi tentang biaya snapshot dan retensinya, lihat harga Amazon EBS.

Sebagai akun GuardDuty administrator yang didelegasikan, hanya Anda yang dapat melakukan pembaruan ini atas nama akun anggota organisasi. Namun, jika akun anggota dikelola dengan metode undangan, mereka dapat membuat perubahan ini sendiri. Untuk informasi selengkapnya, lihat Akun administrator dan hubungan akun anggota.

Pilih metode akses pilihan Anda untuk mengaktifkan pengaturan retensi snapshot.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. Pilih Pengaturan umum di bagian bawah konsol. Untuk mempertahankan snapshot, aktifkan retensi Snapshots.

API/CLI

Jalankan UpdateMalwareScanSettingsuntuk memperbarui konfigurasi saat ini untuk pengaturan retensi snapshot.

Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk menyimpan snapshot secara otomatis saat Perlindungan GuardDuty Malware untuk EC2 menghasilkan temuan.

Pastikan untuk mengganti *`detector-id`* dengan valid Anda sendiri`detectorId`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

Jika Anda ingin mematikan retensi snapshot, ganti `RETENTION_WITH_FINDING` dengan`NO_RETENTION`.

Opsi pindai dengan tag yang ditentukan pengguna

Dengan menggunakan pemindaian GuardDuty-initiated malware, Anda juga dapat menentukan tag untuk menyertakan atau mengecualikan instans Amazon EC2 dan volume Amazon EBS dari proses pemindaian dan deteksi ancaman. Anda dapat menyesuaikan setiap pemindaian GuardDuty-initiated malware dengan mengedit tag di daftar tag penyertaan atau pengecualian. Setiap daftar dapat mencakup hingga 50 tag.

Jika Anda belum memiliki tag yang ditentukan pengguna yang terkait dengan sumber daya EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

> **Note**
>
> On-demand pemindaian malware tidak mendukung opsi pemindaian dengan tag yang ditentukan pengguna. Ini mendukung`GuardDutyExcludedTag` global.

Untuk mengecualikan instans EC2 dari pemindaian malware

Jika Anda ingin mengecualikan instans Amazon EC2 atau volume Amazon EBS selama proses pemindaian, Anda dapat menyetel `GuardDutyExcluded` tag `true` untuk instans Amazon EC2 atau volume Amazon EBS apa pun, GuardDuty dan tidak akan memindainya. Untuk informasi selengkapnya tentang `GuardDutyExcluded` tag, lihatService-linked izin peran untuk Perlindungan Malware untuk EC2. Anda juga dapat menambahkan tag instans Amazon EC2 ke daftar pengecualian. Jika Anda menambahkan beberapa tag ke daftar tag pengecualian, instans Amazon EC2 yang berisi setidaknya satu tag ini akan dikecualikan dari proses pemindaian malware.

Sebagai akun GuardDuty administrator yang didelegasikan, hanya Anda yang dapat melakukan pembaruan ini atas nama akun anggota organisasi. Namun, jika akun anggota dikelola dengan metode undangan, mereka dapat membuat perubahan ini sendiri. Untuk informasi selengkapnya, lihat Akun administrator dan hubungan akun anggota.

Pilih metode akses pilihan Anda untuk menambahkan tag yang terkait dengan instans Amazon EC2, ke daftar pengecualian.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. Perluas bagian Inclusion/Exclusion tag. Pilih Tambahkan tag.
4. Pilih tag Pengecualian dan kemudian pilih untuk Konfirmasi.
5. Tentukan tag **`Key`** dan **`Value`** pasangkan yang ingin Anda kecualikan. Ini opsional untuk menyediakan**`Value`**. Setelah Anda menambahkan semua tag, pilih Simpan.

   > **Important**
   >
   > Kunci dan nilai tanda peka terhadap huruf besar dan kecil. Untuk informasi selengkapnya, lihat Pembatasan tag di Panduan Pengguna Amazon EC2.

   Jika nilai untuk kunci tidak disediakan dan instans EC2 ditandai dengan kunci yang ditentukan, instans EC2 ini akan dikecualikan dari proses pemindaian GuardDuty-initiated malware, terlepas dari nilai yang ditetapkan tag.

API/CLI

Jalankan UpdateMalwareScanSettingsdengan mengecualikan instans EC2 atau beban kerja kontainer dari proses pemindaian.

Perintah AWS CLI contoh berikut menambahkan tag baru ke daftar tag pengecualian. Ganti contoh *`detector-id`* dengan valid Anda sendiri`detectorId`.

`MapEquals`adalah daftar `Key` `Value` /pasangan.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
```

```
"TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
"RETENTION_WITH_FINDING"
```

> **Important**
>
> Kunci dan nilai tanda peka terhadap huruf besar dan kecil. Untuk informasi selengkapnya, lihat Pembatasan tag di Panduan Pengguna Amazon EC2.

Untuk menyertakan instans EC2 dalam pemindaian malware

Jika Anda ingin memindai instans EC2, tambahkan tagnya ke daftar inklusi. Saat Anda menambahkan tag ke daftar tag inklusi, instans EC2 yang tidak berisi tag yang ditambahkan akan dilewati dari pemindaian malware. Jika Anda menambahkan beberapa tag ke daftar tag inklusi, instans EC2 yang berisi setidaknya satu dari tag tersebut disertakan dalam pemindaian malware. Terkadang, instans EC2 dapat dilewati selama proses pemindaian karena alasan lain. Untuk informasi selengkapnya, lihat Alasan melewatkan sumber daya selama pemindaian malware.

Sebagai akun GuardDuty administrator yang didelegasikan, hanya Anda yang dapat melakukan pembaruan ini atas nama akun anggota organisasi. Namun, jika akun anggota dikelola dengan metode undangan, mereka dapat membuat perubahan ini sendiri. Untuk informasi selengkapnya, lihat Akun administrator dan hubungan akun anggota.

Pilih metode akses pilihan Anda untuk menambahkan tag yang terkait dengan instans EC2, ke daftar inklusi.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. Perluas bagian Inclusion/Exclusion tag. Pilih Tambahkan tag.
4. Pilih tag Inklusi dan kemudian pilih Konfirmasi.
5. Pilih Tambahkan tag inklusi baru dan tentukan tag **`Key`** dan **`Value`** pasangan yang ingin Anda sertakan. Ini opsional untuk menyediakan**`Value`**.

   Setelah Anda menambahkan semua tag inklusi, pilih Simpan.

Jika nilai untuk kunci tidak diberikan, instans EC2 ditandai dengan kunci yang ditentukan, instans EC2 akan disertakan dalam proses pemindaian Perlindungan Malware untuk EC2, terlepas dari nilai yang ditetapkan tag.

API/CLI

- Jalankan UpdateMalwareScanSettingsuntuk menyertakan instans EC2 atau beban kerja kontainer dalam proses pemindaian.

  AWS CLI Contoh perintah berikut menambahkan tag baru ke daftar tag inklusi. Pastikan Anda mengganti contoh *detector-id* dengan valid Anda sendiri`detectorId`. Ganti contoh *TestKey* dan *TestValue* dengan `Key` dan `Value` pasangan tag yang terkait dengan sumber daya EC2 Anda.

  `MapEquals`adalah daftar `Key` `Value` /pasangan.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Include":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

  Important

  Kunci dan nilai tanda peka terhadap huruf besar dan kecil. Untuk informasi selengkapnya, lihat Pembatasan tag di Panduan Pengguna Amazon EC2.

Note

Mungkin diperlukan waktu hingga 5 menit GuardDuty untuk mendeteksi tag baru.

Kapan saja, Anda dapat memilih tag Inklusi atau tag Pengecualian tetapi tidak keduanya. Jika Anda ingin beralih di antara tag, pilih tag itu dari menu tarik-turun saat Anda menambahkan tag baru, dan Konfirmasikan pilihan Anda. Tindakan ini menghapus semua tag Anda saat ini.

`GuardDutyExcluded`Tag global

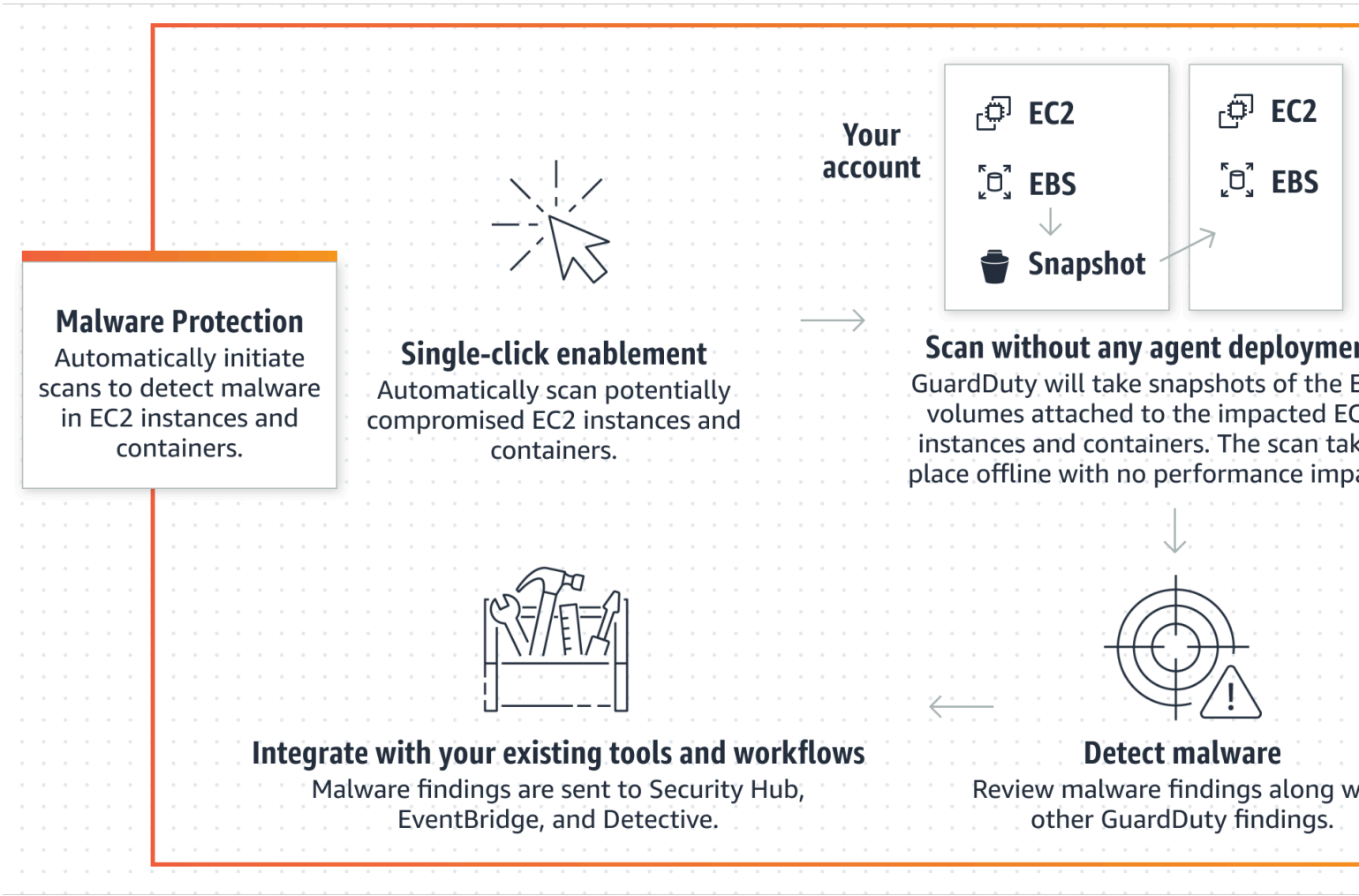
GuardDuty menggunakan kunci tag global,`GuardDutyExcluded`, yang dapat Anda tambahkan ke sumber daya Amazon EC2 Anda dan menetapkan nilai tag ke. `true` Sumber daya Amazon EC2 yang memiliki kunci tag dan pasangan nilai ini akan dikecualikan dari pemindaian malware. Kedua jenis pemindaian (pemindaian GuardDuty-initiated On-demand malware dan pemindaian malware) mendukung tag global. Jika Anda memulai pemindaian malware sesuai permintaan di Amazon EC2, ID pemindaian akan dihasilkan. Namun, pemindaian akan dilewati dengan suatu `EXCLUDED_BY_SCAN_SETTINGS` alasan. Untuk informasi selengkapnya, lihat Alasan melewatkan sumber daya selama pemindaian malware.

GuardDuty-initiated pemindaian malware

Dengan pemindaian GuardDuty-initiated malware diaktifkan, kapan pun GuardDuty menghasilkanTemuan yang memanggil pemindaian GuardDuty-initiated malware, pemindaian malware tanpa agen di volume Amazon Elastic Block Store (Amazon EBS) Elastic Block Store (Amazon EBS) yang dilampirkan ke sumber daya Amazon EC2 yang berpotensi terkena dampak akan dimulai. Sebelum pemindaian dimulai, Anda harus menyiapkan akun Anda untuk penyesuaian apa pun. Dengan opsi pemindaian, Anda dapat menambahkan tag inklusi yang terkait dengan sumber daya yang ingin Anda pindai, atau menambahkan tag pengecualian yang terkait dengan sumber daya yang ingin Anda lewati dari proses pemindaian. Inisiasi pemindaian otomatis akan selalu mempertimbangkan opsi pemindaian Anda. GuardDuty juga mendukung pasangan global`GuardDutyExcluded`: `true` tag key:value. Saat Anda menambahkan tag global ini ke sumber daya Amazon EC2, GuardDuty akan memulai pemindaian dan kemudian melewatinya. Anda juga dapat memilih untuk mengaktifkan pengaturan retensi snapshot untuk mempertahankan snapshot volume EBS Anda di mana malware berpotensi terdeteksi. Untuk informasi selengkapnya tentang opsi pemindaian, tag pengecualian global, dan setelan snapshot, lihat. Mengatur retensi snapshot dan cakupan pemindaian EC2

Ketika GuardDuty menghasilkan beberapa temuan untuk sumber daya Amazon EC2 yang sama, GuardDuty akan dapat memulai pemindaian hanya setelah 24 jam telah berlalu sejak pemindaian malware terakhir GuardDuty-initiated . Untuk informasi tentang bagaimana volume Amazon EBS yang dilampirkan ke instans Amazon EC2 atau beban kerja container dipindai, lihat. Cara GuardDuty memindai volume EBS untuk deteksi malware

Gambar berikut menjelaskan cara kerja pemindaian GuardDuty-initiated malware.



Untuk informasi tentang metodologi deteksi GuardDuty malware dan mesin pemindaian yang digunakannya, lihatGuardDuty mesin pemindai deteksi malware.

Ketika malware ditemukan, GuardDuty hasilkanPerlindungan Malware untuk jenis pencarian EC2. Jika GuardDuty tidak menghasilkan temuan yang menunjukkan malware pada sumber daya yang sama, tidak ada pemindaian GuardDuty-initiated malware yang akan dipanggil. Anda juga dapat memulai pemindaian On-demand malware pada sumber daya yang sama. Untuk informasi selengkapnya, lihat On-demand pemindaian malware GuardDuty.

Uji coba gratis 30 hari dalam pemindaian GuardDuty-initiated malware

Anda dapat memilih untuk mengaktifkan atau menonaktifkan pemindaian GuardDuty-initiated malware untuk file yang didukung Wilayah AWS kapan saja. Akun AWS Jika Anda memiliki organisasi, setiap akun anggota memiliki uji coba gratis 30 hari sendiri.

Untuk memahami cara kerja uji coba gratis 30 hari, pertimbangkan skenario berikut:

- Saat Anda mengaktifkan GuardDuty untuk pertama kalinya (GuardDuty akun baru), pemindaian GuardDuty-initiated malware juga diaktifkan dan disertakan dalam uji coba gratis 30 hari yang terkait dengan GuardDuty layanan.
- GuardDuty Akun yang ada dapat mengaktifkan pemindaian GuardDuty-initiated malware untuk pertama kalinya dengan uji coba gratis 30 hari. Saat Anda mengaktifkan fitur ini di Wilayah yang berbeda untuk pertama kalinya, Anda akan mendapatkan uji coba gratis 30 hari di Wilayah tersebut.
- Jika Anda telah menggunakan Perlindungan Malware untuk EC2 Wilayah AWS sebelum rencana perlindungan ini dibagi menjadi dua jenis pemindaian — pemindaian GuardDuty-initiated malware dan pemindaian On-demand malware, Anda dapat terus menggunakan pemindaian GuardDuty-initiated malware dengan model harga yang sama Wilayah AWS. Jika Anda mengaktifkan pemindaian GuardDuty-initiated malware untuk pertama kalinya di Wilayah baru, akun Anda akan mendapatkan uji coba gratis 30 hari.

> **Note**
>
> Bahkan jika Anda berada dalam masa uji coba gratis 30 hari, biaya penggunaan standar untuk membuat snapshot volume Amazon EBS dan retensinya berlaku. Untuk informasi selengkapnya, lihat harga Amazon EBS.

Mengaktifkan pemindaian GuardDuty-initiated malware di lingkungan beberapa akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang dapat mengaktifkan pemindaian GuardDuty-initiated malware atas nama akun anggota mereka. Selain itu, akun administrator yang mengelola akun anggota dengan AWS Organizations dukungan dapat memilih untuk mengaktifkan pemindaian GuardDuty-initiated malware secara otomatis pada semua akun yang ada dan yang baru di organisasi. Untuk informasi selengkapnya, lihat Mengelola GuardDuty akun dengan AWS Organizations.

Membangun akses tepercaya untuk mengaktifkan pemindaian GuardDuty-initiated malware

Jika akun administrator GuardDuty yang didelegasikan tidak sama dengan akun manajemen di organisasi Anda, akun manajemen harus mengaktifkan pemindaian GuardDuty-initiated malware untuk organisasi mereka. Dengan cara ini, akun administrator yang didelegasikan dapat membuat akun anggota Service-linked izin peran untuk Perlindungan Malware untuk EC2 di yang dikelola. AWS Organizations

> **Note**
>
> Sebelum Anda menetapkan akun GuardDuty administrator yang didelegasikan, lihat. Pertimbangan dan rekomendasi

Pilih metode akses pilihan Anda untuk mengizinkan akun GuardDuty administrator yang didelegasikan mengaktifkan pemindaian GuardDuty-initiated malware untuk akun anggota di organisasi.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Untuk masuk, gunakan akun manajemen untuk AWS Organizations organisasi Anda.

2. a. Jika Anda belum menetapkan akun GuardDuty administrator yang didelegasikan, maka:

      Pada halaman Pengaturan, di bawah akun GuardDuty administrator yang didelegasikan, masukkan 12 digit **`account ID`** yang ingin Anda tetapkan untuk mengelola GuardDuty kebijakan di organisasi Anda. Pilih Delegasikan.

   b. i. Jika Anda telah menetapkan akun GuardDuty administrator yang didelegasikan yang berbeda dari akun manajemen, maka:

         Pada halaman Pengaturan, di bawah Administrator Delegasi, aktifkan pengaturan Izin. Tindakan ini akan memungkinkan akun GuardDuty administrator yang didelegasikan untuk melampirkan izin yang relevan ke akun anggota dan mengaktifkan pemindaian GuardDuty-initiated malware di akun anggota ini.

      ii. Jika Anda telah menetapkan akun GuardDuty administrator yang didelegasikan yang sama dengan akun manajemen, maka Anda dapat langsung mengaktifkan

pemindaian GuardDuty-initiated malware untuk akun anggota. Untuk informasi selengkapnya, lihat Auto-enable GuardDuty-initiated pemindaian malware untuk semua akun anggota.

> **Tip**
>
> Jika akun GuardDuty administrator yang didelegasikan berbeda dari akun manajemen Anda, Anda harus memberikan izin ke akun GuardDuty administrator yang didelegasikan untuk memungkinkan pemindaian GuardDuty-initiated malware untuk akun anggota.

3. Jika Anda ingin mengizinkan akun GuardDuty administrator yang didelegasikan untuk mengaktifkan pemindaian GuardDuty-initiated malware untuk akun anggota di Wilayah lain, ubah Wilayah AWS, dan ulangi langkah-langkah di atas.

API/CLI

1. Menggunakan kredensi akun manajemen Anda, jalankan perintah berikut:

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (Opsional) untuk mengaktifkan pemindaian GuardDuty-initiated malware untuk akun manajemen yang bukan akun administrator yang didelegasikan, akun manajemen pertama-tama akan membuat secara Service-linked izin peran untuk Perlindungan Malware untuk EC2 eksplisit di akun mereka, dan kemudian mengaktifkan pemindaian GuardDuty-initiated malware dari akun administrator yang didelegasikan, mirip dengan akun anggota lainnya.

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. Anda telah menetapkan akun GuardDuty administrator yang didelegasikan dalam yang dipilih Wilayah AWS saat ini. Jika Anda telah menetapkan akun sebagai akun GuardDuty administrator yang didelegasikan di satu wilayah, akun tersebut harus merupakan akun GuardDuty administrator yang didelegasikan di semua wilayah lain. Ulangi langkah di atas untuk semua Wilayah lainnya.

Mengkonfigurasi pemindaian GuardDuty-initiated malware untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan pemindaian GuardDuty-initiated malware untuk akun GuardDuty administrator yang didelegasikan.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
3. Pada halaman Perlindungan Malware untuk EC2, pilih Edit di samping pemindaian GuardDuty-initiated malware.
4. Lakukan salah satu tindakan berikut:

   Penggunaan Aktifkan untuk semua akun

   - Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
   - Pilih Simpan.

   Penggunaan Konfigurasikan akun secara manual

   - Untuk mengaktifkan paket perlindungan hanya untuk akun akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
   - Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
   - Pilih Simpan.

API/CLI

Jalankan operasi updateDetectorAPI menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek `name` sebagai `EBS_MALWARE_PROTECTION` dan `status` sebagai`ENABLED`.

Anda dapat mengaktifkan pemindaian GuardDuty-initiated malware dengan menjalankan AWS CLI perintah berikut. Pastikan untuk menggunakan akun GuardDuty administrator yang didelegasikan valid*`detector ID`*.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Auto-enable GuardDuty-initiated pemindaian malware untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan fitur pemindaian GuardDuty-initiated malware untuk semua akun anggota. Ini termasuk akun anggota yang ada dan akun baru yang bergabung dengan organisasi.

Console

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensil akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu tindakan berikut:

   Menggunakan Perlindungan Malware untuk EC2 halaman

   1. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
   2. Pada halaman Perlindungan Malware untuk EC2, pilih Edit di bagian pemindaian GuardDuty-initiated malware.
   3. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan pemindaian GuardDuty-initiated malware untuk akun yang ada dan baru di organisasi.
   4. Pilih Simpan.

   > **Note**
   >
   > Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Menggunakan Akun halaman

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Auto-enablepreferensi sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah pemindaian GuardDuty-initiated malware.
4. Pada halaman Perlindungan Malware untuk EC2, pilih Edit di bagian pemindaian GuardDuty-initiated malware.
5. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan pemindaian GuardDuty-initiated malware untuk akun yang ada dan baru di organisasi.
6. Pilih Simpan.

> **Note**
>
> Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Menggunakan Akun halaman

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Auto-enablepreferensi sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah pemindaian GuardDuty-initiated malware.
4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun, lihat[Aktifkan pemindaian GuardDuty-initiated malware untuk akun anggota secara selektif](#).

API/CLI

- Untuk mengaktifkan pemindaian GuardDuty-initiated malware secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID*
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan pemindaian GuardDuty-initiated malware untuk satu akun anggota. Untuk menonaktifkan akun anggota, ganti `ENABLED` dengan`DISABLED`.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
  ```

  Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.
- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan pemindaian GuardDuty-initiated malware untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan pemindaian GuardDuty-initiated malware untuk semua akun anggota aktif yang ada di organisasi.

Untuk mengonfigurasi pemindaian GuardDuty-initiated malware untuk semua akun anggota aktif yang ada

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.
2. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
3. Pada Perlindungan Malware untuk EC2, Anda dapat melihat status konfigurasi pemindaian GuardDuty-initiated malware saat ini. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.

5. Pilih Simpan.

Auto-enable GuardDuty-initiated pemindaian malware untuk akun anggota baru

Akun anggota yang baru ditambahkan harus Aktifkan GuardDuty sebelum memilih mengonfigurasi pemindaian GuardDuty-initiated malware. Akun anggota yang dikelola oleh undangan dapat mengonfigurasi pemindaian GuardDuty-initiated malware secara manual untuk akun mereka. Untuk informasi selengkapnya, lihat Step 3 - Accept an invitation.

Pilih metode akses pilihan Anda untuk mengaktifkan pemindaian GuardDuty-initiated malware untuk akun baru yang bergabung dengan organisasi Anda.

Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan pemindaian GuardDuty-initiated malware untuk akun anggota baru dalam suatu organisasi, baik menggunakan halaman Perlindungan Malware untuk EC2 atau Akun.

Untuk mengaktifkan pemindaian GuardDuty-initiated malware secara otomatis untuk akun anggota baru

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensil akun GuardDuty administrator yang didelegasikan.
2. Lakukan salah satu tindakan berikut:
   - Menggunakan halaman Perlindungan Malware untuk EC2:
     1. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
     2. Pada halaman Perlindungan Malware untuk EC2, pilih Edit dalam pemindaian GuardDuty-initiated malware.
     3. Pilih Konfigurasikan akun secara manual.
     4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, pemindaian GuardDuty-initiated malware akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
     5. Pilih Simpan.
   - Menggunakan halaman Akun:

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Auto-enablepreferensi.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah pemindaian GuardDuty-initiated malware.
4. Pilih Simpan.

API/CLI

- Untuk mengaktifkan atau menonaktifkan pemindaian GuardDuty-initiated malware untuk akun anggota baru, jalankan operasi UpdateOrganizationConfigurationAPI menggunakan akun Anda sendiri*detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan pemindaian GuardDuty-initiated malware untuk satu akun anggota. Untuk menonaktifkannya, lihatAktifkan pemindaian GuardDuty-initiated malware untuk akun anggota secara selektif. Jika Anda tidak ingin mengaktifkannya untuk semua akun baru yang bergabung dengan organisasi, setel `AutoEnable` ke`NONE`.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name":
   "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
  ```

  Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.
- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan pemindaian GuardDuty-initiated malware untuk akun anggota secara selektif

Pilih metode akses pilihan Anda untuk mengonfigurasi pemindaian GuardDuty-initiated malware untuk akun anggota secara selektif.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Akun.
3. Pada halaman Akun, tinjau kolom pemindaian GuardDuty-initiated malware untuk status akun anggota Anda.
4. Pilih akun yang ingin Anda konfigurasikan pemindaian GuardDuty-initiated malware. Anda dapat memilih beberapa akun sekaligus.
5. Dari menu Edit paket perlindungan, pilih opsi yang sesuai untuk pemindaian GuardDuty-initiated malware.

API/CLI

Untuk mengaktifkan atau menonaktifkan pemindaian GuardDuty-initiated malware untuk akun anggota Anda secara selektif, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID*

Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan pemindaian GuardDuty-initiated malware untuk satu akun anggota.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
 "Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Untuk mengaktifkan pemindaian GuardDuty-initiated malware secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri*detector ID*. Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan pemindaian GuardDuty-initiated malware untuk satu akun anggota.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan pemindaian GuardDuty-initiated malware untuk akun yang ada di Organisasi yang dikelola melalui undangan

Perlindungan GuardDuty Malware untuk peran terkait layanan EC2 (SLR) harus dibuat di akun anggota. Akun administrator tidak dapat mengaktifkan fitur pemindaian GuardDuty-initiated malware di akun anggota yang tidak dikelola oleh AWS Organizations.

Saat ini, Anda dapat melakukan langkah-langkah berikut melalui GuardDuty konsol di https://console.aws.amazon.com/guardduty/untuk mengaktifkan pemindaian GuardDuty-initiated malware untuk akun anggota yang ada.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Masuk menggunakan kredensi akun administrator Anda.
2. Di panel navigasi, pilih Akun.
3. Pilih akun anggota yang ingin Anda aktifkan pemindaian GuardDuty-initiated malware. Anda dapat memilih beberapa akun sekaligus.
4. Pilih Tindakan.
5. Pilih anggota Disassociate.
6. Di akun anggota Anda, pilih Perlindungan Malware di bawah Paket Perlindungan di panel navigasi.

7. Pilih Aktifkan pemindaian GuardDuty-initiated malware. GuardDuty akan membuat SLR untuk akun anggota. Untuk informasi lebih lanjut tentang SLR, lihatService-linked izin peran untuk Perlindungan Malware untuk EC2.
8. Di akun akun administrator Anda, pilih Akun di panel navigasi.
9. Pilih akun anggota yang perlu ditambahkan kembali ke organisasi.
10. Pilih Tindakan dan kemudian, pilih Tambah anggota.

API/CLI

1. Gunakan akun akun administrator untuk menjalankan DisassociateMembersAPI pada akun anggota yang ingin mengaktifkan pemindaian GuardDuty-initiated malware.
2. Gunakan akun anggota Anda untuk memanggil UpdateDetectoruntuk mengaktifkan pemindaian GuardDuty-initiated malware.

   Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

   ```
   aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
   {"EbsVolumes":true}}}'
   ```
3. Gunakan akun akun administrator untuk menjalankan CreateMembersAPI guna menambahkan anggota kembali ke organisasi.

Mengaktifkan pemindaian GuardDuty-initiated malware untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat Mengaktifkan pemindaian GuardDuty-initiated malware di lingkungan beberapa akun.

Setelah Anda mengaktifkan pemindaian GuardDuty-initiated malware, GuardDuty akan memulai pemindaian malware dari volume Amazon EBS yang dilampirkan ke instans Amazon EC2 yang terlibat dalam file. GuardDuty Untuk daftar temuan yang memulai pemindaian malware, lihatTemuan yang memanggil pemindaian GuardDuty-initiated malware.

Pilih metode akses pilihan Anda untuk mengonfigurasi pemindaian GuardDuty-initiated malware untuk akun mandiri.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. Panel Perlindungan Malware untuk EC2 mencantumkan status pemindaian GuardDuty-initiated malware saat ini untuk akun Anda. Pilih Aktifkan untuk mengaktifkan pemindaian GuardDuty-initiated malware di akun ini.
4. Pilih Simpan untuk mengonfirmasi pilihan Anda.

API/CLI

Jalankan operasi updateDetectorAPI menggunakan ID detektor regional Anda sendiri dan teruskan `dataSources` objek dengan `EbsVolumes` disetel `ketrue`.

Anda juga dapat mengaktifkan pemindaian GuardDuty-initiated malware menggunakan AWS CLI dengan menjalankan AWS CLI perintah berikut. Pastikan untuk menggunakan valid Anda sendiri*detector ID*.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
 aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]'
```

Temuan yang memanggil pemindaian GuardDuty-initiated malware

Ketika GuardDuty mendeteksi perilaku mencurigakan yang menunjukkan malware pada instans Amazon EC2 atau beban kerja container yang berjalan pada instans Amazon EC2, akan menghasilkan temuan. GuardDuty Jika temuan yang dihasilkan ini termasuk dalam daftar GuardDuty temuan berikut, maka secara otomatis GuardDuty akan memulai pemindaian malware pada volume Amazon EBS yang melekat pada instans Amazon EC2 yang terlibat dalam temuan tersebut. Setelah scan, jika GuardDuty mendeteksi malware, maka itu juga akan menghasilkan satu atau lebihPerlindungan Malware untuk jenis pencarian EC2.

Jika salah satu GuardDuty temuan berikut dihasilkan di akun Anda, secara otomatis GuardDuty akan memulai pemindaian malware dalam volume Amazon EBS dari instans Amazon EC2 yang berpotensi dikompromikan.

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:Runtime/PtraceAntiDebugging
- DefenseEvasion:Runtime/SuspiciousCommand
- Execution:Runtime/MaliciousFileExecuted
- Execution:Runtime/MaliciousFileExecuted.Custom
- Execution:Runtime/SuspiciousCommand
- Execution:Runtime/SuspiciousShellCreated
- Execution:Runtime/SuspiciousTool
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce(Hanya keluar)
- PrivilegeEscalation:Runtime/ElevationToRoot
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic

- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/RDPBruteForce(Hanya keluar)
- UnauthorizedAccess:EC2/SSHBruteForce(Hanya keluar)
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay
- Backdoor:Runtime/C&CActivity.B
- Backdoor:Runtime/C&CActivity.B! DNS
- CryptoCurrency:Runtime/BitcoinTool.B
- CryptoCurrency:Runtime/BitcoinTool.B! DNS
- Execution:Runtime/NewBinaryExecuted
- Execution:Runtime/NewLibraryLoaded
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/CryptoMinerExecuted
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape

- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/BlackholeTraffic! DNS
- Trojan:Runtime/DropPoint
- Trojan:Runtime/DropPoint! DNS
- Trojan:Runtime/DGADomainRequest.C! DNS
- Trojan:Runtime/DriveBySourceTraffic! DNS
- Trojan:Runtime/PhishingDomainRequest! DNS
- UnauthorizedAccess:Runtime/MetadataDNSRebind

On-demand pemindaian malware GuardDuty

On-demand pemindaian malware membantu Anda mendeteksi keberadaan malware di volume Amazon Elastic Block Store (Amazon EBS) yang dilampirkan ke instans Amazon EC2 Anda. Tanpa konfigurasi yang diperlukan, Anda dapat memulai pemindaian malware sesuai permintaan dengan memberikan Nama Sumber Daya Amazon (ARN) dari instans Amazon EC2 yang ingin Anda pindai. Anda dapat memulai pemindaian malware sesuai permintaan baik melalui GuardDuty konsol atau API. Sebelum memulai pemindaian malware sesuai permintaan, Anda dapat mengatur pengaturan pilihan Retensi snapshot Anda. Skenario berikut dapat membantu Anda mengidentifikasi kapan harus menggunakan jenis pemindaian On-demand malware dengan GuardDuty:

- Anda ingin mendeteksi keberadaan malware di instans Amazon EC2 Anda tanpa mengaktifkan GuardDuty-initiated pemindaian malware.
- Anda telah mengaktifkan pemindaian GuardDuty-initiated malware dan pemindaian dipanggil secara otomatis. Setelah mengikuti perbaikan yang disarankan untuk jenis pencarian Perlindungan Malware yang dihasilkan untuk EC2, jika Anda ingin memulai pemindaian pada sumber daya yang sama, Anda dapat memulai pemindaian malware sesuai permintaan setelah 1 jam berlalu dari waktu mulai pemindaian sebelumnya.

  On-demand Pemindaian malware tidak mengharuskan 24 jam telah berlalu sejak pemindaian malware sebelumnya dimulai. Seharusnya satu jam berlalu sebelum memulai pemindaian On-demand malware pada sumber daya yang sama. Untuk menghindari duplikasi pemindaian malware pada instans EC2 yang sama, lihat. Re-scanning instans Amazon EC2 yang sebelumnya dipindai

> **Note**
>
> On-demand Pemindaian malware tidak termasuk dalam periode uji coba gratis 30 hari dengan GuardDuty. Biaya penggunaan berlaku untuk total volume Amazon EBS yang dipindai untuk setiap pemindaian malware. Untuk informasi selengkapnya, lihat GuardDuty harga Amazon. Untuk informasi tentang biaya pembuatan snapshot volume Amazon EBS dan retensinya, lihat harga Amazon EBS.

Cara kerja pemindaian On-demand malware

Dengan pemindaian On-demand malware, Anda dapat memulai permintaan pemindaian malware untuk instans Amazon EC2 Anda bahkan saat sedang digunakan. Setelah Anda memulai pemindaian On-demand malware, GuardDuty buat snapshot volume Amazon EBS yang dilampirkan ke instans Amazon EC2 yang Nama Sumber Daya Amazon (ARN) disediakan untuk pemindaian. Selanjutnya, GuardDuty bagikan foto-foto ini dengan. GuardDuty akun layanan GuardDuty membuat volume EBS replika terenkripsi dari snapshot tersebut di akun layanan. GuardDuty Untuk informasi selengkapnya tentang bagaimana volume Amazon EBS dipindai, lihat. Cara GuardDuty memindai volume EBS untuk deteksi malware

> **Note**
>
> GuardDuty membuat snapshot dari data yang telah ditulis ke volume Amazon EBS pada saat Anda memulai pemindaian malware. On-demand

Jika malware ditemukan dan Anda telah mengaktifkan pengaturan retensi snapshot, snapshot volume EBS Anda secara otomatis disimpan di Anda. Akun AWS On-demand pemindaian malware menghasilkanPerlindungan Malware untuk jenis pencarian EC2. Jika malware tidak ditemukan, maka terlepas dari pengaturan retensi snapshot, snapshot volume EBS Anda akan dihapus.

GuardDuty menggunakan kunci tag global,`GuardDutyExcluded`, yang dapat Anda tambahkan ke sumber daya Amazon EC2 Anda dan menetapkan nilai tag ke. `true` Sumber daya Amazon EC2 yang memiliki kunci tag dan pasangan nilai ini akan dikecualikan dari pemindaian malware. Kedua jenis pemindaian (pemindaian GuardDuty-initiated On-demand malware dan pemindaian malware) mendukung tag global. Jika Anda memulai pemindaian malware sesuai permintaan di Amazon EC2, ID pemindaian akan dihasilkan. Namun, pemindaian akan dilewati dengan suatu

`EXCLUDED_BY_SCAN_SETTINGS` alasan. Untuk informasi selengkapnya, lihat Alasan melewatkan sumber daya selama pemindaian malware.

Memulai pemindaian On-demand malware di GuardDuty

Bagian ini menyediakan daftar prasyarat sebelum memulai pemindaian malware sesuai permintaan dan langkah-langkah untuk memulai pemindaian pada sumber daya untuk pertama kalinya.

Sebagai akun GuardDuty administrator, Anda dapat memulai pemindaian malware sesuai permintaan atas nama akun anggota aktif Anda yang memiliki prasyarat berikut di akun mereka. Akun mandiri dan akun anggota aktif juga GuardDuty dapat memulai pemindaian malware sesuai permintaan untuk instans Amazon EC2 mereka sendiri.

Prasyarat

Sebelum Anda memulai pemindaian On-demand malware, akun Anda harus memenuhi prasyarat berikut:

- GuardDuty harus diaktifkan di Wilayah AWS tempat Anda ingin memulai pemindaian malware sesuai permintaan.
- Pastikan bahwa AWS kebijakan yang dikelola: AmazonGuardDutyFullAccess_v2 (direkomendasikan) terpasang ke pengguna IAM atau peran IAM. Anda akan memerlukan kunci akses dan kunci rahasia yang terkait dengan pengguna IAM atau peran IAM.
- Sebagai akun GuardDuty administrator yang didelegasikan, Anda memiliki opsi untuk memulai pemindaian malware sesuai permintaan atas nama akun anggota yang aktif.
- Sebelum Anda memulai pemindaian malware sesuai permintaan, pastikan tidak ada pemindaian yang dimulai pada sumber daya yang sama dalam 1 jam terakhir; jika tidak, itu akan dihapus. Untuk informasi selengkapnya, lihat Re-scanning instans Amazon EC2 yang sebelumnya dipindai.
- Jika Anda adalah akun anggota yang tidak memilikinyaService-linked izin peran untuk Perlindungan Malware untuk EC2, maka memulai pemindaian malware sesuai permintaan untuk instans Amazon EC2 milik akun Anda, akan secara otomatis membuat SLR untuk Perlindungan Malware untuk EC2.

> **Important**
>
> Pastikan tidak ada yang menghapus izin SLR untuk Perlindungan Malware untuk EC2 saat pemindaian malware masih berlangsung. Pemindaian malware ini dapat dimulai oleh

GuardDuty atau dimulai sesuai permintaan. Menghapus SLR akan mencegah pemindaian selesai dengan sukses, dan memberikan hasil pemindaian yang pasti.

Mulai pemindaian On-demand malware

Anda dapat memulai pemindaian malware sesuai permintaan di akun Anda melalui GuardDuty konsol atau dengan menggunakan AWS CLI. Anda harus memberikan Amazon EC2 Amazon Resource Name (ARN) yang ingin Anda mulai pemindaian. Langkah-langkah terperinci disediakan di konsol dan AWS CLI API/instruksi di bagian berikut.

Pilih metode akses pilihan Anda untuk memulai pemindaian malware sesuai permintaan.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Mulai pemindaian menggunakan salah satu opsi berikut:
   a. Menggunakan halaman Perlindungan Malware untuk EC2:
      i. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
      ii. Pada halaman Perlindungan Malware untuk EC2, berikan instans Amazon EC2 ARN 1 yang ingin Anda mulai pemindaian.
   b. Menggunakan halaman Pemindaian Malware:
      i. Di panel navigasi, pilih Pemindaian Malware.
      ii. Pilih Mulai pemindaian sesuai permintaan dan berikan instans Amazon EC2 ARN 1 yang ingin Anda mulai pemindaian.
      iii. Jika ini adalah pemindaian ulang, pilih ID instans Amazon EC2 di halaman Pemindaian Malware.

      Perluas tarik-turun pemindaian Mulai sesuai permintaan dan pilih instance yang dipilihRe-scan .
3. Setelah Anda berhasil memulai pemindaian menggunakan salah satu metode, ID pemindaian akan dihasilkan. Anda dapat menggunakan ID pemindaian ini untuk melacak kemajuan pemindaian. Untuk informasi selengkapnya, lihat Memantau status dan hasil pemindaian malware.

API/CLI

Invoke StartMalwareScanyang menerima [instans] Amazon EC2 1 yang Anda inginkan untuk memulai pemindaian malware sesuai permintaan. `resourceArn`

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

Setelah Anda berhasil memulai pemindaian, `StartMalwareScan` mengembalikan file`scanId`. DescribeMalwareScansMemanggil memantau kemajuan pemindaian yang dimulai.

[1] Untuk informasi tentang format ARN instans Amazon EC2 Anda, lihat Nama Sumber Daya Amazon (ARN). Untuk instans Amazon EC2, Anda dapat menggunakan contoh format ARN berikut dengan mengganti nilai untuk partisi, Wilayah, ID, Akun AWS dan ID instans Amazon EC2. Untuk informasi tentang panjang ID instans Anda, lihat ID Sumber Daya.

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

AWS Organizations kebijakan kontrol layanan - Akses ditolak

Dengan menggunakan kebijakan kontrol Layanan (SCP) di AWS Organizations, akun GuardDuty administrator yang didelegasikan dapat membatasi izin dan menolak tindakan seperti memulai pemindaian malware sesuai permintaan untuk instans Amazon EC2 yang dimiliki oleh akun Anda.

Sebagai akun GuardDuty anggota, saat Anda memulai pemindaian malware sesuai permintaan untuk instans Amazon EC2 Anda, Anda mungkin menerima kesalahan. Anda dapat terhubung dengan akun manajemen untuk memahami mengapa SCP disiapkan untuk akun anggota Anda. Untuk informasi selengkapnya, lihat efek SCP pada izin.

Re-scanning instans Amazon EC2 yang sebelumnya dipindai

Baik pemindaian GuardDuty-initiated atau dimulai sesuai permintaan, Anda dapat memulai pemindaian malware sesuai permintaan baru pada instans Amazon EC2 yang sama setelah 1 jam dari waktu mulai pemindaian malware sebelumnya. Jika pemindaian malware baru dimulai dalam waktu 1 jam setelah inisiasi pemindaian malware sebelumnya, permintaan Anda akan menghasilkan kesalahan berikut, dan tidak ada ID pemindaian yang akan dihasilkan untuk permintaan ini.

```
A scan was started on this resource recently. You can request a scan on the
same resource one hour after the previous scan start time.
```

Langkah-langkah untuk memindai ulang instance tetap sama dengan memulai pemindaian malware sesuai permintaan untuk pertama kalinya. Untuk informasi tentang langkah-langkahnya, lihatMulai pemindaian On-demand malware.

Untuk melacak status pemindaian malware, lihatMemantau status pemindaian dan hasil dalam Perlindungan Malware untuk EC2.

Memantau status pemindaian dan hasil dalam Perlindungan Malware untuk EC2

Setelah pemindaian malware dimulai pada instans Amazon EC2 GuardDuty , berikan bidang status dan hasil secara otomatis. Anda dapat memantau status melalui transisi, dan melihat apakah malware terdeteksi. Tabel berikut memberikan nilai yang mungkin terkait dengan pemindaian malware.

Nilai potensial
`Running`,`Completed` ,`Skipped`, atau `Failed`
`Clean` atau `Infected`
`GuardDuty initiated` atau `On demand`

* Hasil pemindaian hanya diisi ketika status pemindaian menjadi. `Completed` Hasil pemindaian `Infected` berarti GuardDuty mendeteksi keberadaan malware.

Hasil pemindaian untuk setiap pemindaian malware memiliki periode retensi 90 hari. Pilih metode akses pilihan Anda untuk melacak status pemindaian malware Anda.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih pemindaian malware EC2.
3. Anda dapat memfilter pemindaian malware dengan Properti berikut yang tersedia di bilah pencarian filter.

   - Scan ID — Pengidentifikasi unik yang terkait dengan pemindaian malware EC2.
   - ID Akun — Akun AWS ID tempat pemindaian malware dimulai.
   - ARN instans EC2 — Nama Sumber Daya Amazon (ARN) yang terkait dengan instans Amazon EC2 yang terkait dengan pemindaian.
   - Status pemindaian — Status pemindaian volume EBS, seperti Running, Skipped, dan Completed
   - Jenis pemindaian - Menunjukkan apakah ini pemindaian On-demand malware atau pemindaian GuardDuty-initiated malware.

API/CLI

- Setelah pemindaian malware memiliki hasil pemindaian, gunakan DescribeMalwareScansuntuk memfilter pemindaian malware berdasarkan`EC2_INSTANCE_ARN`,,`SCAN_ID`,`ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`SCAN_STATUS, dan`SCAN_START_TIME`.

  Kriteria `GUARDDUTY_FINDING_ID` filter `SCAN_TYPE` tersedia saat GuardDuty dimulai.

- Anda dapat mengubah contoh pada perintah *`filter-criteria`* di bawah ini. Saat ini, Anda dapat memfilter berdasarkan satu `CriterionKey` per satu. Pilihan untuk `CriterionKey` adalah`EC2_INSTANCE_ARN`,`SCAN_ID`,`ACCOUNT_ID`, `SCAN_TYPE`GUARDDUTY_FINDING_ID,`SCAN_STATUS`, dan`SCAN_START_TIME`.

  Anda dapat mengubah *`max-results`* (hingga 50) dan*`sort-criteria`*. `AttributeName`Itu wajib dan harus`scanStartTime`.

  Dalam contoh berikut, nilai-nilai di *`red`* adalah placeholder. Ganti dengan nilai yang sesuai untuk akun Anda. Misalnya, ganti contoh `detector-id` *`60b87779336485625 54d637e0e4bb3b2`* dengan valid Anda sendiri`detector-id`. Jika Anda menggunakan yang sama `CriterionKey` seperti di bawah ini, pastikan untuk mengganti contoh `EqualsValue` dengan valid Anda sendiri AWS *`scan-id`*.

```
aws guardduty describe-malware-scans --detector-
id 60b87779336485625554d637e0e4bb3b2 --max-results 1 --sort-criteria
 '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
{"EqualsValue":"123456789012"}}] }'
```

- Respons dari perintah ini menampilkan maksimal satu hasil dengan rincian tentang sumber daya yang terpengaruh dan temuan malware (jika`Infected`).

GuardDuty akun layanan oleh Wilayah AWS

Saat snapshot dibuat dan dibagikan dengan akun GuardDuty layanan, acara baru akan dibuat di CloudTrail log Anda. Acara ini menentukan yang sesuai `snapshotId` dan `userId` (akun GuardDuty layanan untuk itu Wilayah AWS). Untuk informasi selengkapnya, lihat Cara GuardDuty memindai volume EBS untuk deteksi malware.

Contoh berikut adalah cuplikan dari CloudTrail peristiwa yang menunjukkan badan permintaan untuk permintaan: `ModifySnapshotAttribute`

```
"requestParameters": {
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

Tabel berikut menunjukkan akun GuardDuty layanan untuk setiap Wilayah. `userId`Ini adalah akun GuardDuty layanan dan tergantung pada Wilayah yang dipilih.

Wilayah AWS	Kode Wilayah	GuardDuty ID akun layanan (**`userId`**)
AS Timur (Virginia Utara)	us-east-1	652050842985

Wilayah AWS	Kode Wilayah	GuardDuty ID akun layanan (**`userId`**)
AS Timur (Ohio)	us-east-2	178123968615
AS Barat (California Utara)	us-west-1	669213148797
AS Barat (Oregon)	us-west-2	447226417196
Asia Pasifik (Mumbai)	ap-south-1	913179291432
Asia Pasifik (Osaka)	ap-northeast-3	089661699081
Asia Pasifik (Seoul)	ap-northeast-2	039163547507
Asia Pasifik (Tokyo)	ap-northeast-1	874749492622
Asia Pasifik (Singapura)	ap-southeast-1	247460962669
Asia Pasifik (Sydney)	ap-southeast-2	124839743349
Kanada (Pusat)	ca-central-1	175877067165
Kanada Barat (Calgary)	ca-west-1	894794104037
Eropa (Frankfurt)	eu-central-1	002294850712
Eropa (Irlandia)	eu-west-1	283769539786
Eropa (London)	eu-west-2	310125036783
Eropa (Paris)	eu-west-3	866607715269
Eropa (Stockholm)	eu-north-1	693780578038
Tiongkok (Beijing)	cn-north-1	448721096076
Tiongkok (Ningxia)	cn-northwest-1	480864352451
Amerika Selatan (Sao Paulo)	sa-east-1	546914126324

Wilayah AWS	Kode Wilayah	GuardDuty ID akun layanan (**`userId`**)
Asia Pasifik (Hyderabad) () Opt-in	ap-south-2	682251015962
Asia Pasifik (Melbourne) (Opt-in)	ap-southeast-4	353488359550
Asia Pasifik (Malaysia) (Opt-in)	ap-southeast-5	009160069308
Asia Pasifik (Thailand) (Opt-in)	ap-southeast-7	941377115582
Eropa (Spanyol) Opt-in ()	eu-south-2	936182149045
Eropa (Zurich) () Opt-in	eu-central-2	867642063380
Israel (Tel Aviv) (Opt-in)	il-central-1	619233833001
Europe (Milan) (Opt-in)	eu-south-1	977238331021
Asia Pacific (Hong Kong) (Opt-in)	ap-east-1	249472122084
Middle East (Bahrain) (Opt-in)	me-south-1	404001805210
Africa (Cape Town) (Opt-in)	af-south-1	957664736811
Asia Pasifik (Jakarta) (Opt-in)	ap-southeast-3	452118225523
Timur Tengah (UEA) (Opt-in)	me-central-1	828603743433
Meksiko (Tengah) Opt-in ()	mx-central-1	557690616787

Wilayah AWS	Kode Wilayah	GuardDuty ID akun layanan (**`userId`**)
Asia Pasifik (Taipei)	ap-east-2	863518437308
Asia Pasifik (Selandia Baru)	ap-southeast-6	686255982852
AWS GovCloud (US-East)	us-gov-east-1	226283551151
AWS GovCloud (US-West)	us-gov-west-1	226300430612

Kuota dalam Perlindungan Malware untuk EC2

Bagian ini mencakup kuota yang terkait dengan penggunaan Perlindungan Malware untuk EC2. Untuk kuota yang terkait dengan GuardDuty, lihatGuardDuty kuota.

Tabel berikut menyediakan ketersediaan default berbagai sumber daya saat Anda menggunakan Perlindungan Malware untuk EC2.

Lingkup	Bawaan	Komentar
Ekstraksi dan analisis data dalam file terkompresi atau diarsipkan	5	Jumlah maksimum level bersarang yang diizinkan dalam file yang diarsipkan.
Jumlah file dalam file yang diarsipkan	1000	Jumlah maksimum file yang dapat dipindai dalam arsip. Hitungan ini adalah jumlah dari jumlah file yang diekstrak dari arsip dan jumlah file yang diekstrak dari semua arsip bersarang.
Jumlah Ancaman	32	Jumlah maksimum ancaman yang dapat Anda lihat di panel temuan. GuardDuty

Lingkup	Bawaan	Komentar
		Perlindungan Malware untuk EC2 mungkin telah mendeteksi lebih banyak nama ancaman. Jika jumlah nama ancaman yang terdeteksi lebih tinggi dari nilai default, Anda dapat melihat detail JSON dengan memilih ID Menemukan di bawah nama temuan di panel detail GuardDuty konsol.
Jumlah file per ancaman yang terdeteksi	5	Jumlah maksimum file yang diidentifikasi per ancaman yang terdeteksi. Misalnya, jika GuardDuty mendeteksi 10 file yang terkait dengan ancaman tunggal, ancaman akan menampilkan maksimal 5 file.
Volume EBS per pemindaian per instance	11	Jumlah maksimum volume EBS yang GuardDuty dapat memindai per instans EC2. Jika ada lebih dari 11 volume EBS yang perlu dipindai, Perlindungan GuardDuty Malware untuk EC2 mengurutkan `deviceName` berdasarkan abjad, dan memilih 11 volume EBS pertama.

Lingkup	Bawaan	Komentar
Ukuran volume EBS	2048 GB	Terkait dengan instans Amazon EC2 dan beban kerja kontainer, Perlindungan GuardDuty Malware untuk EC2 dapat memindai setiap volume Amazon EBS yang berukuran hingga 2048 GB. Kuota ini berlaku untuk masing-masing Wilayah AWS tempat dukungan untuk Perlindungan Malware untuk EC2 tersedia.
Jenis sistem file yang didukung	GuardDuty Perlindungan Malware untuk EC2 dapat memindai jenis sistem file berikut: • Sistem File Teknologi Baru (NTFS) • Sistem File X (XFS) • Sistem File kedua diperpanjang (ext2) • Sistem File diperpanjang keempat (ext4) • Sistem File Tabel Alokasi File (FAT) • Sistem File Tabel Alokasi File Virtual (VFAT)	N/A.

Lingkup	Bawaan	Komentar
Tag opsi pindai	50	Jumlah maksimum tag sumber daya yang dapat Anda tambahkan untuk menyesuaikan pengaturan opsi pemindaian malware Anda. Untuk informasi selengkapnya, lihat Opsi pindai dengan tag yang ditentukan pengguna.
Menemukan periode retensi	90	Jumlah hari maksimum yang GuardDuty mempertahankan temuan. Untuk informasi terbaru, lihatGuardDuty Kuota Amazon.
Periode retensi pemindaian malware	90	Jumlah hari maksimum Perlindungan GuardDuty Malware untuk EC2 mempertahankan riwayat pemindaian. Untuk informasi selengkapnya tentang melihat pemindaian malware terbaru, lihatMemantau status pemindaian dan hasil dalam Perlindungan Malware untuk EC2.
Transaksi per detik (TPS) untuk pemindaian On-demand malware	1	Jumlah permintaan pemindaian On-demand malware yang dapat dimulai per detik di setiap Wilayah.

Lingkup	Bawaan	Komentar
Batas burst untuk pemindaian On-demand malware	1	Jumlah permintaan pemindaian malware On-demand malware bersamaan yang dapat dimulai per detik di setiap Wilayah.

GuardDuty Perlindungan Malware untuk S3

Perlindungan Malware untuk S3 membantu Anda mendeteksi potensi keberadaan malware dengan memindai objek yang baru diunggah ke bucket Amazon Simple Storage Service (Amazon S3) pilihan Anda. Ketika objek S3 atau versi baru dari objek S3 yang ada diunggah ke bucket yang Anda pilih, GuardDuty secara otomatis memulai pemindaian malware.

Perlindungan Malware untuk S3 - Ikhtisar dan Demo

Dua pendekatan untuk mengaktifkan Perlindungan Malware untuk S3

Anda dapat mengaktifkan Perlindungan Malware untuk S3 ketika Anda Akun AWS mengaktifkan GuardDuty layanan dan Anda menggunakan Perlindungan Malware untuk S3 sebagai bagian dari keseluruhan GuardDuty pengalaman, atau ketika Anda ingin menggunakan fitur Perlindungan Malware untuk S3 dengan sendirinya tanpa mengaktifkan layanan. GuardDuty Saat Anda mengaktifkan Perlindungan Malware untuk S3 dengan sendirinya, GuardDuty dokumentasi merujuknya sebagai menggunakan Perlindungan Malware untuk S3 sebagai fitur independen.

Pertimbangan untuk menggunakan Perlindungan Malware untuk S3 secara independen

- GuardDuty temuan keamanan — Detector ID adalah pengenal unik yang dikaitkan dengan akun Anda di Wilayah. Ketika Anda mengaktifkan GuardDuty di satu atau beberapa Wilayah

dalam akun, ID detektor akan dibuat secara otomatis untuk akun ini di setiap Wilayah tempat Anda mengaktifkan GuardDuty. Untuk informasi selengkapnya, lihat Detektor dalam Konsep dan istilah kunci di Amazon GuardDuty dokumen.

Saat Anda mengaktifkan Perlindungan Malware untuk S3 secara independen di akun, akun tersebut tidak akan memiliki ID detektor terkait. Ini memengaruhi GuardDuty fitur apa yang mungkin tersedia untuk Anda. Misalnya, ketika pemindaian malware S3 mendeteksi keberadaan malware, tidak ada GuardDuty temuan yang akan dihasilkan di Anda Akun AWS karena semua GuardDuty temuan terkait dengan ID detektor.

- Memeriksa apakah objek yang dipindai berbahaya — Secara default, GuardDuty mempublikasikan hasil pemindaian malware ke bus EventBridge acara Amazon default Anda dan namespace Amazon CloudWatch . Saat Anda mengaktifkan penandaan pada saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket, objek S3 yang dipindai mendapatkan tag yang menyebutkan hasil pemindaian. Untuk informasi lebih lanjut tentang penandaan, lihat Penandaan opsional objek berdasarkan hasil pemindaian.

Pertimbangan umum untuk mengaktifkan Perlindungan Malware untuk S3

Pertimbangan umum berikut berlaku apakah Anda menggunakan Perlindungan Malware untuk S3 secara independen atau sebagai bagian dari GuardDuty pengalaman:

- Anda dapat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3 milik akun Anda sendiri. Sebagai akun GuardDuty administrator yang didelegasikan, Anda tidak dapat mengaktifkan fitur ini di bucket Amazon S3 milik akun anggota.
- Anda dapat mengaktifkan fitur ini di bucket S3 milik Wilayah yang sama yang saat ini dipilih di GuardDuty konsol. GuardDuty tidak mendukung pengaktifan fitur ini di bucket S3 lintas wilayah.
- Sebagai akun GuardDuty administrator yang didelegasikan, Anda akan menerima EventBridge notifikasi Amazon setiap kali ada perubahan pada bucket S3 yang dikonfigurasi oleh salah satu akun anggota organisasi Anda untuk fitur ini. Melihat dan memahami status bucket yang dilindungi

Konten

- Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3
- Bagaimana cara kerja Perlindungan Malware untuk S3?
- Kemampuan Perlindungan Malware untuk S3
- (Opsional) Memulai Perlindungan GuardDuty Malware untuk S3 secara independen (hanya konsol)
- Mengkonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda

- Langkah-langkah setelah mengaktifkan Perlindungan Malware untuk S3
- On-demand Pemindaian malware S3 masuk GuardDuty
- Menggunakan kontrol akses berbasis tag (TBAC) dengan Perlindungan Malware untuk S3
- Melihat dan memahami status bucket yang dilindungi
- Memantau pemindaian objek S3 di Perlindungan Malware untuk S3
- Pemecahan Masalah
- Mengedit paket Perlindungan Malware untuk bucket yang dilindungi
- Menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi
- Dukungan fitur Amazon S3
- Kuota dalam Perlindungan Malware untuk S3

Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3

Harga dalam Perlindungan Malware untuk S3 bekerja secara berbeda dari paket perlindungan lainnya di GuardDuty. Sementara sebagian besar paket GuardDuty perlindungan mengikuti uji coba gratis jangka pendek 30 hari, Perlindungan Malware untuk S3 menyertakan Tingkat Gratis. AWS Untuk informasi tentang GuardDuty harga, lihatHarga di GuardDuty.

Daftar berikut memberikan biaya harga yang terkait dengan penggunaan Perlindungan Malware untuk S3.

Tingkat Gratis (biaya pemindaian)

Masing-masing Akun AWS mendapat Tingkat Gratis yang mencakup penggunaan hingga batas tertentu per bulan untuk setiap Wilayah. Masing-masing Akun AWS mendapat penggunaan tingkat gratis bulanan hingga 1.000 permintaan dan data 1 GB dipindai. Jika penggunaan Anda melampaui batas yang ditentukan, Anda akan mulai mengeluarkan biaya penggunaan untuk batas yang terlampaui. Untuk detail harga lengkap, lihat harga paket GuardDuty perlindungan.

> **Important**
>
> On-demand pemindaian tidak termasuk dalam tingkat gratis.

Untuk informasi tentang biaya penggunaan setelah mengaktifkan Perlindungan Malware untuk S3, lihat. Meninjau biaya penggunaan untuk Perlindungan Malware untuk S3

Biaya penggunaan Penandaan Objek S3

Saat Anda mengaktifkan Perlindungan Malware untuk S3, itu opsional untuk mengaktifkan penandaan untuk objek S3 yang dipindai. Ketika Anda memilih untuk mengaktifkan S3 Object Tagging, ada biaya penggunaan terkait. Untuk informasi selengkapnya tentang biaya, lihat tab Manajemen & wawasan di halaman harga Amazon S3.

Biaya penggunaan Penandaan Objek S3 tidak termasuk dalam Tingkat Gratis.

API Amazon S3 - GET dan biaya penggunaan PUT

Anda akan dikenakan biaya penggunaan saat GuardDuty menjalankan API Amazon S3 berdasarkan peran IAM. Misalnya, setelah mengasumsikan peran IAM, GuardDuty jalankan `PutObject` API untuk menambahkan objek pengujian ke bucket yang Anda pilih. Ini membantu GuardDuty menilai status fitur yang diaktifkan.

Untuk informasi tentang harga panggilan API S3 di Anda Wilayah AWS, lihat Permintaan & pengambilan data di bawah tab Penyimpanan & permintaan di halaman harga Amazon S3.

Biaya penggunaan API Amazon S3 tidak termasuk dalam Tingkat Gratis.

EventBridge Biaya Aturan Terkelola

GuardDuty menggunakan aturan EventBridge terkelola untuk mendeteksi kapan objek baru diunggah ke bucket yang dilindungi. Anda akan dikenakan biaya untuk acara keikutsertaan Amazon S3 yang dicerna oleh. EventBridge Anda tidak akan dikenakan biaya pengiriman acara. Untuk informasi tentang EventBridge harga, lihat EventBridge harga.

EventBridge Biaya Aturan Terkelola tidak termasuk dalam Tingkat Gratis.

Meninjau biaya penggunaan untuk Perlindungan Malware untuk S3

Akun Anda mulai mengeluarkan biaya penggunaan saat Anda menggunakan Perlindungan Malware untuk S3 di luar batas spesifik di bawah Tingkat Gratis. Untuk informasi tentang Tingkat Gratis, lihatHarga dan biaya penggunaan untuk Perlindungan Malware untuk S3. Perhatikan bahwa Tingkat Gratis tidak berlaku untuk Perlindungan Malware untuk pemindaian objek sesuai permintaan S3.

GuardDuty Konsol tidak mendukung peninjauan Perlindungan Malware untuk biaya penggunaan S3. Untuk melihat biaya penggunaan, navigasikan ke Cost Explorer di https://console.aws.amazon.com/

costmanagement/konsol. Untuk informasi tentang Akun AWS penagihan, lihat Panduan AWS Billing Pengguna.

Untuk informasi tentang perkiraan biaya penggunaan GuardDuty, lihatMemantau penggunaan dan memperkirakan biaya.

Bagaimana cara kerja Perlindungan Malware untuk S3?

Bagian ini menjelaskan komponen Perlindungan Malware untuk S3, cara kerjanya setelah Anda mengaktifkannya untuk bucket S3, dan bagaimana Anda dapat meninjau status dan hasil pemindaian malware.

Gambaran umum

Anda dapat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3 milik Anda sendiri. Akun AWS GuardDutymemberi Anda fleksibilitas untuk mengaktifkan fitur ini untuk seluruh bucket Anda, atau membatasi cakupan pemindaian malware ke awalan objek tertentu tempat GuardDuty memindai konten setiap objek yang diunggah yang dimulai dengan salah satu awalan yang dipilih. Anda dapat menambahkan hingga 5 awalan. Saat Anda mengaktifkan fitur untuk bucket S3, bucket tersebut disebut bucket yang dilindungi.

Izin peran IAM

Perlindungan Malware untuk S3 menggunakan peran IAM yang memungkinkan GuardDuty untuk melakukan tindakan pemindaian malware atas nama Anda. Tindakan ini termasuk diberi tahu tentang objek yang baru diunggah di bucket yang dipilih, memindai objek tersebut, dan secara opsional menambahkan tag ke objek yang dipindai. Ini adalah prasyarat untuk mengonfigurasi bucket S3 Anda dengan fitur ini.

Anda memiliki opsi untuk memperbarui peran IAM yang ada, atau membuat peran baru untuk tujuan ini. Saat mengaktifkan Perlindungan Malware untuk S3 untuk lebih dari satu bucket, Anda dapat memperbarui peran IAM yang ada untuk menyertakan nama bucket lainnya, sesuai kebutuhan. Untuk informasi selengkapnya, lihat Membuat atau memperbarui kebijakan peran IAM.

Penandaan opsional objek berdasarkan hasil pemindaian

Pada saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda, ada langkah opsional untuk mengaktifkan penandaan objek S3 yang dipindai. Peran IAM sudah menyertakan izin untuk

menambahkan tag ke objek Anda setelah pemindaian. Namun, GuardDuty akan menambahkan tag hanya ketika Anda mengaktifkan opsi ini pada saat setup.

Anda harus mengaktifkan opsi ini sebelum objek diunggah. Setelah pemindaian berakhir, GuardDuty tambahkan tag yang telah ditentukan ke objek S3 yang dipindai dengan pasangan key:value berikut:

`GuardDutyMalwareScanStatus:`*`Potential scan result`*

Nilai tag hasil pemindaian potensial meliputi`NO_THREATS_FOUND`,`THREATS_FOUND`,`UNSUPPORTED`,`ACCESS_DENIED`, dan`FAILED`. Untuk informasi selengkapnya tentang nilai-nilai ini, lihatthe section called “Status pemindaian potensial objek S3 dan status hasil”.

Mengaktifkan penandaan adalah salah satu cara untuk mengetahui tentang hasil pemindaian objek S3. Anda dapat menggunakan tag ini lebih lanjut untuk menambahkan kebijakan sumber daya S3 kontrol akses berbasis tag (TBAC) sehingga Anda dapat mengambil tindakan pada objek yang berpotensi berbahaya. Untuk informasi selengkapnya, lihat Menambahkan TBAC pada sumber daya bucket S3.

Kami menyarankan Anda untuk mengaktifkan penandaan pada saat mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda. Jika Anda mengaktifkan penandaan setelah objek diunggah dan berpotensi pemindaian dimulai, tidak GuardDuty akan dapat menambahkan tag ke objek yang dipindai. Untuk informasi tentang biaya Penandaan Objek S3 terkait, lihat. Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3

Proses setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk ember

Setelah Anda mengaktifkan Perlindungan Malware untuk S3, sumber daya paket Perlindungan Malware akan dibuat secara eksklusif untuk bucket S3 yang dipilih. Sumber daya ini dikaitkan dengan ID paket Perlindungan Malware, pengenal unik untuk sumber daya Anda yang dilindungi. Dengan menggunakan salah satu izin IAM, GuardDuty kemudian membuat dan mengelola aturan EventBridge terkelola dengan nama. `DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*`

Bagaimana GuardDuty menangani data Anda - pagar pembatas untuk perlindungan data

Perlindungan Malware untuk S3 mendengarkan notifikasi Amazon EventBridge . Saat objek diunggah ke bucket yang dipilih atau salah satu awalan, GuardDuty unduh objek tersebut dari bucket S3

dengan menggunakan lalu membaca, mendekripsi, AWS PrivateLinkdan memindainya di lingkungan terisolasi di Wilayah yang sama. Lingkungan pemindaian berjalan di cloud pribadi virtual (VPC) yang terkunci tanpa akses internet. VPC dilampirkan ke grup aturan DNS Firewall yang memungkinkan komunikasi hanya ke domain allowslisted yang dimiliki. AWS Selama pemindaian, simpan GuardDuty sementara objek S3 yang diunduh dalam lingkungan pemindaian yang dienkripsi dengan kunci AWS Key Management Service ()AWS KMS.

> **Note**
>
> Secara default, semua API Amazon S3 yang tercantum di bawah jenis Peristiwa yang Dibuat Objek di Panduan Pengguna Amazon S3, akan memulai Perlindungan Malware untuk pemindaian S3.
> Jenis Event ini termasuk PutObject, POST Object CopyObject, dan CompleteMultipartUpload.

Untuk informasi tentang metodologi deteksi GuardDuty malware dan mesin pemindaian yang digunakannya, lihatGuardDuty mesin pemindai deteksi malware.

Setelah pemindaian malware selesai, GuardDuty proses metadata pemindaian dengan status pemindaian dan kemudian menghapus salinan objek yang diunduh.

GuardDuty membersihkan lingkungan pemindaian setiap kali sebelum pemindaian baru dimulai. GuardDuty menggunakan otorisasi kontingen untuk akses operator ke lingkungan pemindaian, dan setiap permintaan akses ditinjau, disetujui, dan diaudit.

Meninjau status dan hasil pemindaian objek S3

GuardDuty menerbitkan peristiwa hasil pemindaian objek S3 ke bus acara EventBridge default Amazon. GuardDuty juga mengirimkan metrik pemindaian seperti jumlah objek yang dipindai dan byte yang dipindai ke Amazon. CloudWatch Jika Anda mengaktifkan penandaan, maka GuardDuty akan menambahkan tag yang telah ditentukan `GuardDutyMalwareScanStatus` dan hasil pemindaian potensial sebagai nilai tag.

> **Important**
>
> GuardDuty menggunakan pengiriman paling tidak sekali, yang berarti Anda mungkin menerima beberapa hasil pemindaian untuk objek yang sama. Kami merekomendasikan merancang aplikasi Anda untuk menangani hasil duplikat. Anda hanya ditagih sekali untuk setiap objek yang dipindai.

Untuk informasi selengkapnya, lihat Memantau pemindaian objek S3 di Perlindungan Malware untuk S3.

Meninjau temuan yang dihasilkan

Meninjau temuan tergantung pada apakah Anda menggunakan Perlindungan Malware untuk S3 dengan atau tidak. GuardDuty Pertimbangkan skenario berikut:

Menggunakan Perlindungan Malware untuk S3 ketika Anda mengaktifkan GuardDuty layanan (ID detektor)

- Jika pemindaian malware mendeteksi file yang berpotensi berbahaya di objek S3, GuardDuty akan menghasilkan temuan terkait. Anda dapat melihat detail temuan dan menggunakan langkah-langkah yang disarankan untuk berpotensi memulihkan temuan tersebut. Berdasarkan frekuensi temuan Ekspor Anda, temuan yang dihasilkan akan diekspor ke bucket S3 dan bus EventBridge acara.

  Untuk informasi tentang jenis temuan yang akan dihasilkan, lihatPerlindungan Malware untuk tipe pencarian S3.

Menggunakan Perlindungan Malware untuk S3 sebagai fitur independen (tidak ada ID detektor)

- GuardDuty tidak akan dapat menghasilkan temuan karena tidak ada ID detektor terkait. Untuk mengetahui status pemindaian malware objek S3, Anda dapat melihat hasil pemindaian yang GuardDuty secara otomatis dipublikasikan ke bus acara default Anda. Anda juga dapat melihat CloudWatch metrik untuk menilai jumlah objek dan byte yang GuardDuty mencoba memindai. Anda dapat mengatur CloudWatch alarm untuk mendapatkan pemberitahuan tentang hasil pemindaian. Jika Anda telah mengaktifkan S3 Object Tagging, Anda juga dapat melihat status pemindaian malware dengan memeriksa objek S3 untuk kunci `GuardDutyMalwareScanStatus` tag dan nilai tag hasil pemindaian.

  Untuk informasi tentang status dan hasil pemindaian objek S3, lihatMemantau pemindaian objek S3 di Perlindungan Malware untuk S3.

Kemampuan Perlindungan Malware untuk S3

Daftar berikut memberikan ikhtisar tentang apa yang dapat Anda harapkan atau lakukan setelah mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda:

- Pilih apa yang akan dipindai — Pindai file saat diunggah ke semua atau awalan tertentu (hingga 5) yang terkait dengan bucket S3 pilihan Anda.
- Pemindaian otomatis pada objek yang diunggah — Setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk ember, secara otomatis GuardDuty akan memulai pemindaian untuk mendeteksi potensi malware di objek yang baru diunggah.
- On-demand pemindaian — Anda dapat memulai pemindaian untuk objek yang ada atau memindai ulang objek yang sebelumnya dipindai. Untuk informasi selengkapnya, lihat On-demand Pemindaian malware S3 masuk GuardDuty.
- Aktifkan melalui konsol, dengan menggunakan API/AWS CLI, atau CloudFormation — Pilih metode yang disukai untuk mengaktifkan Perlindungan Malware untuk S3.

  Anda dapat mengaktifkan Perlindungan Malware untuk S3 dengan menggunakan platform Infrastructure as code (IAc) seperti Terraform. Untuk informasi selengkapnya, lihat Sumber Daya: `aws_guardduty_malware_protection_plan`.
- Format file yang didukung, Perlindungan Malware untuk kuota S3, dan fitur Amazon S3 - Perlindungan Malware untuk S3 mendukung semua format file yang dapat Anda unggah ke bucket S3. Jika file yang diunggah dilindungi kata sandi dan GuardDuty mampu mendeteksi keberadaan perlindungan kata sandi untuk jenis file yang diunggah, maka GuardDuty akan mencoba memindai konten asli menggunakan kata sandi umum. Jika kata sandi gagal, pemindaian akan dilewati. GuardDuty tidak dapat mendeteksi keberadaan perlindungan kata sandi pada semua format file. Jika tidak GuardDuty dapat mendeteksi keberadaan proteksi kata sandi, maka GuardDuty akan tetap memindai konten terenkripsi.

  Untuk informasi tentang kuota yang terkait dengan ukuran objek, tingkat kedalaman arsip maksimum, dan detail lainnya, lihatKuota dalam Perlindungan Malware untuk S3.

  Untuk informasi tentang apakah fitur Amazon S3 didukung atau tidak, lihat. Dukungan fitur Amazon S3
- Mendukung penandaan objek S3 yang dipindai - Ketika Anda mengaktifkanPenandaan opsional objek berdasarkan hasil pemindaian, maka setelah setiap pemindaian malware, GuardDuty akan menambahkan tag yang menunjukkan status pemindaian. Anda dapat menggunakan tag ini untuk mengatur kontrol akses berbasis tag (TBAC) untuk objek S3. Misalnya, Anda dapat membatasi akses ke objek S3 yang diindikasikan sebagai berbahaya dan memiliki nilai tag sebagai. `THREATS_FOUND`
- EventBridge Pemberitahuan Amazon — GuardDuty mengirimkan peristiwa ke Amazon EventBridge saat status sumber daya paket Perlindungan Malware berubah, atau pemindaian

malware objek S3 selesai. Peristiwa ini dikirim ke bus acara default. Anda dapat menggunakan EventBridge dan peristiwa ini untuk menulis aturan yang mengambil tindakan, seperti memantau kapan peristiwa ini terjadi. Untuk informasi selengkapnya, lihat Memantau pemindaian objek S3 dengan Amazon EventBridge.

- CloudWatch metrik — Lihat CloudWatch metrik untuk mengaktifkan alarm pada status pemindaian malware tertentu. Lihat informasi yang lebih lengkap di Metrik status pemindaian objek S3 di CloudWatch.

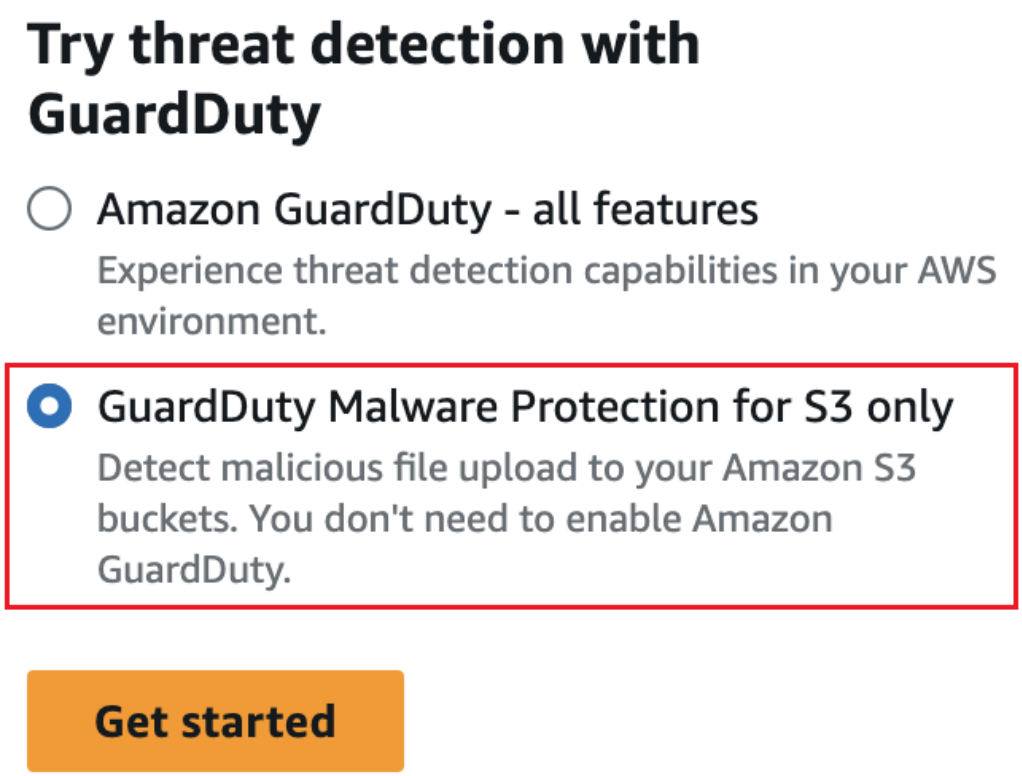
(Opsional) Memulai Perlindungan GuardDuty Malware untuk S3 secara independen (hanya konsol)

Gunakan langkah opsional ini ketika Anda ingin memulai dengan Perlindungan Malware untuk opsi deteksi ancaman S3 terlepas dari GuardDuty status di Anda Akun AWS.

Jika Anda juga ingin menggunakan paket perlindungan khusus lainnya di GuardDuty, Anda harus memulai dengan GuardDuty layanan Amazon. Untuk informasi tentang rencana GuardDuty perlindungan, lihatFitur GuardDuty. Ketika Anda telah mengaktifkan GuardDuty di akun Anda, maka Anda dapat melewati langkah ini dan melanjutkan denganMengkonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda.

Langkah-langkah untuk memulai dengan Perlindungan Malware untuk deteksi ancaman S3 saja

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Pilih Perlindungan GuardDuty Malware hanya untuk S3. Ini membantu Anda mendeteksi apakah file yang baru diunggah di bucket Amazon Simple Storage Service (Amazon S3) berpotensi mengandung malware.



3. Pilih Mulai. Anda sekarang dapat melanjutkan dengan langkah-langkah di bawahMengkonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda.

Mengkonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda

Agar Perlindungan Malware untuk S3 dapat memindai dan (opsional) menambahkan tag ke objek S3 Anda, Anda dapat menggunakan peran layanan yang memiliki izin yang diperlukan untuk melakukan tindakan pemindaian malware atas nama Anda. Untuk informasi selengkapnya tentang menggunakan peran layanan untuk mengaktifkan perlindungan malware untuk S3, lihat Ak ses Layanan. Peran ini berbeda dari peran terkait GuardDuty layanan Perlindungan Malware.

Jika Anda lebih suka menggunakan peran IAM, Anda dapat melampirkan peran IAM yang menyertakan izin yang diperlukan untuk memindai dan (opsional) menambahkan tag ke objek S3 Anda. GuardDuty kemudian mengambil peran IAM ini untuk melakukan tindakan ini atas nama Anda. Anda memerlukan nama peran IAM ini pada saat mengaktifkan paket perlindungan ini untuk bucket Amazon S3 Anda.

Jika Anda menggunakan peran IAM, untuk setiap kali Anda ingin melindungi bucket Amazon S3, Anda harus melakukan kedua langkah yang tercantum di bagian ini.

Untuk mengaktifkan Perlindungan Malware untuk S3, Anda memerlukan detail seperti nama bucket S3, awalan objek jika Anda ingin memfokuskan perlindungan untuk awalan tertentu, dan nama peran IAM dengan izin yang diperlukan.

Langkah-langkah tetap sama apakah Anda memulai dengan Malware Protection untuk S3 secara independen atau mengaktifkannya sebagai bagian dari GuardDuty layanan.

Topik

1. Membuat atau memperbarui kebijakan peran IAM
2. Mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda
3. Memecahkan masalah kesalahan izin peran IAM

Mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda

Bagian ini memberikan langkah-langkah terperinci tentang cara mengaktifkan Perlindungan Malware untuk S3 untuk bucket di akun Anda sendiri. Sebelum Anda melanjutkan, tinjau pertimbangan berikut:

- Saat Anda mengaktifkan paket perlindungan ini menggunakan GuardDuty konsol, paket tersebut mencakup langkah untuk membuat peran baru atau menggunakan peran yang ada di bawah bagian Akses layanan.
- Ketika Anda mengaktifkan paket perlindungan ini menggunakan GuardDuty API atau CLI, maka Anda harus Membuat atau memperbarui kebijakan peran IAM sebelum melanjutkan lebih lanjut.
- Terlepas dari bagaimana Anda mengaktifkan paket perlindungan ini, Anda harus memiliki yang diperlukanIzin untuk membuat sumber daya paket Perlindungan Malware.

Mempertimbangkan pelambatan bucket Amazon S3

S3 Throttling mungkin membatasi kecepatan transfer data ke atau dari bucket Amazon S3 Anda. Ini berpotensi menunda pemindaian malware dari objek yang baru Anda unggah.

Jika Anda mengharapkan volume `GET` dan `PUT` permintaan yang tinggi ke bucket S3 Anda, pertimbangkan untuk menerapkan langkah-langkah untuk mencegah pelambatan. Untuk informasi tentang cara melakukannya, lihat Mencegah pelambatan Amazon S3 di Panduan Pengguna Amazon Athena.

Izin untuk membuat sumber daya paket Perlindungan Malware

Saat Anda mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3, GuardDuty buat sumber daya paket Perlindungan Malware yang bertindak sebagai pengidentifikasi untuk paket perlindungan bucket. Jika Anda belum menggunakanAWS kebijakan yang dikelola: AmazonGuardDutyFullAccess_v2 (direkomendasikan), maka Anda harus menambahkan izin berikut untuk membuat sumber daya ini:

- `guardDuty:CreateMalwareProtectionPlan`
- `iam:PassRole`

Anda dapat menggunakan contoh kebijakan kustom berikut dan menggantinya *`placeholder values`* dengan nilai yang sesuai untuk akun Anda:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/role-name",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateMalwareProtectionPlan"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Mengaktifkan Perlindungan Malware untuk S3 dengan menggunakan GuardDuty konsol

Bagian berikut memberikan panduan langkah demi langkah seperti yang akan Anda alami di GuardDuty konsol.

Untuk mengaktifkan Perlindungan Malware untuk S3 dengan menggunakan GuardDuty konsol

Masukkan detail bucket S3

Gunakan langkah-langkah berikut untuk memberikan detail bucket Amazon S3:

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Dengan menggunakan pem Wilayah AWS ilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengaktifkan Perlindungan Malware untuk S3.
3. Di panel navigasi, pilih Per lindungan Malware untuk S3.
4. Di bagian Bucket yang dilindungi, pilih Akti fkan untuk mengaktifkan Perlindungan Malware untuk S3 untuk bucket S3 milik Anda sendiri Akun AWS.
5. Di bawah Masukkan detail bucket S3, masukkan nama bucket Amazon S3. Atau, pilih Browse S3 untuk memilih bucket S3.

   Buc Wilayah AWS ket S3 dan Akun AWS tempat Anda mengaktifkan Perlindungan Malware untuk S3 harus sama. Misalnya, jika akun Anda milik Wil `us-east-1` ayah, maka Wilayah bucket Amazon S3 Anda juga harus ada`us-east-1`.
6. Di bawah Awalan, Anda dapat memilih Semua objek di bucket S3 atau Ob jek yang dimulai dengan awalan tertentu.

   - Pilih Semua objek di bucket S3 bila Anda mau GuardDuty dapat memindai semua objek yang baru diunggah di bucket yang dipilih.
   - Pilih Objek yang dimulai dengan awalan tertentu ketika Anda ingin memindai objek yang baru diunggah yang termasuk dalam awalan tertentu. Opsi ini membantu Anda memfokuskan cakupan pemindaian malware pada awalan objek yang dipilih saja. Untuk informasi selengkapnya tentang menggunakan awalan, lihat Mengatur objek di konsol Amazon S3 dengan menggunakan folder di Panduan Pengguna Amazon S3.

Pilih Tambahkan awalan dan masukkan awalan. Anda dapat menambahkan hingga lima prefiks.

Aktifkan penandaan untuk objek yang dipindai

Ini adalah langkah opsional. Ketika Anda mengaktifkan opsi penandaan sebelum objek diunggah ke bucket Anda, maka setelah menyelesaikan pemindaian, GuardDuty akan menambahkan tag yang telah ditentukan dengan kunci as `GuardDutyMalwareScanStatus` dan nilai sebagai hasil pemindaian. Untuk menggunakan Perlindungan Malware untuk S3 secara optimal, kami sarankan untuk mengaktifkan opsi untuk menambahkan tag ke objek S3 setelah pemindaian berakhir. Biaya Penandaan Objek S3 Standar berlaku. Untuk informasi selengkapnya, lihat Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3.

Mengapa Anda harus mengaktifkan penandaan?

- Mengaktifkan penandaan adalah salah satu cara untuk mengetahui tentang hasil pemindaian malware. Untuk informasi tentang hasil pemindaian malware S3, lihatMemantau pemindaian objek S3 di Perlindungan Malware untuk S3.
- Siapkan kebijakan kontrol akses berbasis tag (TBAC) pada bucket S3 Anda yang berisi objek yang berpotensi berbahaya. Untuk informasi tentang pertimbangan dan cara menerapkan kontrol akses berbasis tag (TBAC), lihat. Menggunakan kontrol akses berbasis tag (TBAC) dengan Perlindungan Malware untuk S3

Pertimbangan GuardDuty untuk menambahkan tag ke objek S3 Anda:

- Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek. Untuk informasi selengkapnya, lihat Mengkategorikan penyimpanan Anda menggunakan tag di Panduan Pengguna Amazon S3.

  Jika semua 10 tag sudah digunakan, tidak GuardDuty dapat menambahkan tag yang telah ditentukan sebelumnya ke objek yang dipindai. GuardDuty juga menerbitkan hasil pemindaian ke bus EventBridge acara default Anda. Untuk informasi selengkapnya, lihat Memantau pemindaian objek S3 dengan Amazon EventBridge.
- Jika peran IAM yang dipilih tidak menyertakan izin GuardDuty untuk menandai objek S3, maka bahkan dengan penandaan diaktifkan untuk bucket yang dilindungi, tidak GuardDuty akan dapat menambahkan tag ke objek S3 yang dipindai ini. Untuk informasi selengkapnya tentang izin peran IAM yang diperlukan untuk penandaan, lihat. Membuat atau memperbarui kebijakan peran IAM

GuardDuty juga menerbitkan hasil pemindaian ke bus EventBridge acara default Anda. Untuk informasi selengkapnya, lihat Memantau pemindaian objek S3 dengan Amazon EventBridge.

Untuk memilih opsi di bawah Tag objek yang dipindai

- Bila Anda ingin GuardDuty menambahkan tag ke objek S3 yang dipindai, pilih Tag object.
- Jika Anda tidak ingin menambahkan tag GuardDuty ke objek S3 yang dipindai, pilih Jangan menandai objek.

Akses layanan

Gunakan langkah-langkah berikut untuk memilih peran layanan yang ada atau membuat peran layanan baru yang memiliki izin yang diperlukan untuk melakukan tindakan pemindaian malware atas nama Anda. Tindakan ini mungkin termasuk memindai objek S3 yang baru diunggah dan (opsional) menambahkan tag ke objek tersebut. Untuk informasi tentang izin yang akan dimiliki peran ini, lihatMembuat atau memperbarui kebijakan peran IAM.

Di bagian Akses layanan, Anda dapat melakukan salah satu hal berikut:

1. Membuat dan menggunakan peran layanan baru — Anda dapat menggunakan membuat peran layanan baru yang memiliki izin yang diperlukan untuk melakukan pemindaian malware.

   Di bawah nama Peran, Anda dapat memilih untuk menggunakan nama yang telah diisi sebelumnya GuardDuty atau memasukkan nama bermakna pilihan Anda untuk mengidentifikasi peran. Sebagai contoh, `GuardDutyS3MalwareScanRole`. Nama Peran harus terdiri dari 1-64 karakter. Karakter yang valid adalah karakter a-z,, 0-9 A-Z, dan '+=, .@-_'.
2. Menggunakan peran layanan yang ada — Anda dapat memilih peran layanan yang ada dari daftar nama peran layanan.

   a. Di bawah Template Kebijakan, Anda dapat melihat kebijakan untuk bucket S3 Anda. Pastikan Anda memasukkan atau memilih bucket S3 di bagian Masukkan detail bucket S3.

   b. Di bawah Nama peran layanan pilih peran layanan dari daftar peran layanan.

Anda dapat membuat perubahan pada kebijakan berdasarkan persyaratan Anda Untuk detail selengkapnya tentang cara membuat atau memperbarui peran IAM, lihat Membuat atau memperbarui kebijakan peran IAM.

Untuk masalah dengan izin peran IAM, lihatMemecahkan masalah kesalahan izin peran IAM.

(Opsional) Tag ID paket Perlindungan Malware

Ini adalah langkah opsional yang membantu Anda menambahkan tag ke sumber daya paket Perlindungan Malware yang akan dibuat untuk sumber daya bucket S3 Anda.

Setiap tag memiliki dua bagian: kunci tag dan nilai tag opsional. Untuk informasi selengkapnya tentang penandaan dan manfaatnya, lihat Men andai sumber daya AWS .

Untuk menambahkan tag ke sumber daya paket Perlindungan Malware

1. Masukkan Kunci dan Nilai opsional untuk tag. Kunci tag dan nilai tag peka huruf besar-kecil. Untuk informasi tentang nama kunci tag dan nilai tag, lihat Batas dan persyaratan penamaan tag.
2. Untuk menambahkan lebih banyak tag ke sumber daya paket Perlindungan Malware Anda, pilih Tambahkan tag baru dan ulangi langkah sebelumnya. Anda dapat menambahkan hingga 50 tanda ke setiap sumber daya .
3. Pilih Aktifkan.

Mengaktifkan Perlindungan Malware untuk S3 dengan menggunakan API/CLI

Bagian ini mencakup langkah-langkah ketika Anda ingin mengaktifkan Perlindungan Malware untuk S3 secara terprogram di lingkungan Anda AWS . Ini membutuhkan peran IAM Nama Sumber Daya Amazon (ARN) yang Anda buat pada langkah ini -Membuat atau memperbarui kebijakan peran IAM.

Untuk mengaktifkan Perlindungan Malware untuk S3 secara terprogram dengan menggunakan API/CLI

- Dengan menggunakan API

  Jalan CreateMalwareProtectionPlan kan untuk mengaktifkan Perlindungan Malware untuk S3 untuk bucket milik akun Anda sendiri.

- Dengan menggunakan AWS CLI

  Bergantung pada bagaimana Anda ingin mengaktifkan Perlindungan Malware untuk S3, daftar berikut memberikan AWS CLI contoh perintah untuk kasus penggunaan tertentu. Saat Anda menjalankan perintah ini, ganti*`placeholder examples shown in red`*, dengan nilai yang sesuai untuk akun Anda.

AWS CLI contoh perintah

- Gunakan AWS CLI perintah berikut untuk mengaktifkan Perlindungan Malware untuk S3 untuk bucket tanpa penandaan untuk objek S3 yang dipindai:

```
aws guardduty create-malware-protection-plan --role
 "arn:aws:iam::111122223333:role/role-name" --protected-resource
 "S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"}
```

- Gunakan AWS CLI perintah berikut untuk mengaktifkan Perlindungan Malware untuk S3 untuk bucket dengan awalan objek tertentu dan tanpa penandaan untuk objek S3 yang dipindai:

```
aws guardduty create-malware-protection-plan --role
 "arn:aws:iam::111122223333:role/role-name" --protected-resource '{"S3Bucket":
{"BucketName":"amzn-s3-demo-bucket1", "ObjectPrefixes": ["Object1","Object1"]}}'
```

- Gunakan AWS CLI perintah berikut untuk mengaktifkan Perlindungan Malware untuk S3 untuk bucket dengan penandaan objek S3 yang dipindai diaktifkan:

```
aws guardduty create-malware-protection-plan --role
 "arn:aws:iam::111122223333:role/role-name" --protected-resource
 "S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"} --actions
 "Tagging"={"Status"="ENABLED"}
```

Setelah Anda menjalankan perintah ini dengan sukses, ID paket Perlindungan Malware yang unik akan dihasilkan. Untuk melakukan tindakan seperti memperbarui atau menonaktifkan paket perlindungan untuk bucket Anda, Anda memerlukan ID paket Perlindungan Malware ini.

Untuk masalah dengan izin peran IAM, lihatMemecahkan masalah kesalahan izin peran IAM.

Membuat atau memperbarui kebijakan peran IAM

Agar Perlindungan Malware untuk S3 dapat memindai dan (opsional) menambahkan tag ke objek S3 Anda, Anda dapat menggunakan peran layanan yang memiliki izin yang diperlukan untuk melakukan tindakan pemindaian malware atas nama Anda. Untuk informasi selengkapnya tentang menggunakan peran layanan untuk mengaktifkan perlindungan malware untuk S3, lihat Ak ses Layanan. Peran ini berbeda dari peran terkait GuardDuty layanan Perlindungan Malware.

Jika Anda lebih suka menggunakan peran IAM, Anda dapat melampirkan peran IAM yang menyertakan izin yang diperlukan untuk memindai dan (opsional) menambahkan tag ke objek S3 Anda. Anda harus membuat peran IAM atau memperbarui peran yang ada untuk menyertakan izin ini. Karena izin ini diperlukan untuk setiap bucket Amazon S3 yang Anda aktifkan Perlindungan Malware untuk S3, Anda perlu melakukan langkah ini untuk setiap bucket Amazon S3 yang ingin Anda lindungi.

Daftar berikut menjelaskan bagaimana izin tertentu membantu GuardDuty melakukan pemindaian malware atas nama Anda:

- Izinkan EventBridge tindakan Amazon untuk membuat dan EventBridge mengelola aturan terkelola sehingga Perlindungan Malware untuk S3 dapat mendengarkan pemberitahuan objek S3 Anda.

  Untuk informasi selengkapnya, lihat aturan EventBridge yang dikelola Amazon di Panduan EventBridge Pengguna Amazon.
- Izinkan Amazon S3 dan EventBridge tindakan untuk mengirim notifikasi EventBridge untuk semua acara di bucket ini

  Untuk informasi selengkapnya, lihat Meng EventBridge aktifkan Amazon di Panduan Pengguna Amazon S3.
- Izinkan tindakan Amazon S3 untuk mengakses objek S3 yang diunggah dan menambahkan tag yang telah ditentukan sebelumnya,`GuardDutyMalwareScanStatus`, ke objek S3 yang dipindai. Saat menggunakan awalan objek, tambahkan `s3:prefix` kondisi pada awalan yang ditargetkan saja. Ini GuardDuty mencegah mengakses semua objek S3 di bucket Anda.
- Izinkan tindakan kunci KMS untuk mengakses objek sebelum memindai dan menempatkan objek uji pada bucket dengan dukungan DSSE-KMS dan en SSE-KMS kripsi.

> **Note**
>
> Langkah ini diperlukan setiap kali Anda mengaktifkan Perlindungan Malware untuk S3 untuk bucket di akun Anda. Jika Anda sudah memiliki peran IAM, Anda dapat memperbarui kebijakannya untuk menyertakan detail sumber daya bucket Amazon S3 lainnya. Top Menambahkan izin kebijakan IAM ik ini memberikan contoh tentang cara melakukan ini.

Gunakan kebijakan berikut untuk membuat atau memperbarui peran IAM.

Kebijakan

- Menambahkan izin kebijakan IAM
- Menambahkan kebijakan hubungan kepercayaan

Menambahkan izin kebijakan IAM

Anda dapat memilih untuk memperbarui kebijakan sebaris dari peran IAM yang ada, atau membuat peran IAM baru. Untuk informasi tentang langkah-langkahnya, lihat Membuat peran IAM atau M emodifikasi kebijakan izin peran di Panduan Pengguna IAM.

Tambahkan template izin berikut ke peran IAM pilihan Anda. Ganti nilai placeholder berikut dengan nilai yang sesuai terkait dengan akun Anda:

- Untuk*amzn-s3-demo-bucket*, ganti dengan nama bucket Amazon S3 Anda.

  Untuk menggunakan peran IAM yang sama untuk lebih dari satu sumber daya bucket S3, perbarui kebijakan yang ada seperti yang ditampilkan dalam contoh berikut:

  ```
  ...
  ...
  "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "arn:aws:s3:::amzn-s3-demo-bucket2/*"
  ],
  ...
  ...
  ```

  Pastikan untuk menambahkan koma (,) sebelum menambahkan ARN baru yang terkait dengan bucket S3. Lakukan ini di mana pun Anda merujuk ke bucket S3 `Resource` di template kebijakan.
- Untuk*111122223333*, ganti dengan Akun AWS ID Anda.
- Untuk*us-east-1*, ganti dengan Anda Wilayah AWS.
- Untuk*APKAEIBAERJR2EXAMPLE*, ganti dengan ID kunci yang dikelola pelanggan Anda. Jika bucket S3 Anda dienkripsi dengan menggunakan AWS KMS kunci, kami menambahkan izin yang relevan jika Anda memilih opsi Buat peran baru saat mengonfigurasi perlindungan malware untuk bucket Anda.

  ```
  "Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
  ```

Templat kebijakan peran IAM

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ],
            "Condition": {
                "StringLike": {
                    "events:ManagedBy": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
            "Effect": "Allow",
            "Action": [
                "events:DescribeRule",
                "events:ListTargetsByRule"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ]
        },
        {
            "Sid": "AllowPostScanTag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
```

```
                "s3:GetObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:GetObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowEnableS3EventBridgeEvents",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketNotification",
                "s3:GetBucketNotification"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Sid": "AllowPutValidationObject",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-
validation-object"
            ]
        },
        {
            "Sid": "AllowCheckBucketOwnership",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
           "Sid": "AllowMalwareScan",
            "Effect": "Allow",
            "Action": [
```

```
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowDecryptForMalwareScan",
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-
east-1:111122223333:key/APKAEIBAERJR2EXAMPLE",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                }
            }
        }
    ]
}
```

Menambahkan kebijakan hubungan kepercayaan

Lampirkan kebijakan kepercayaan berikut ke peran IAM Anda. Untuk informasi tentang langkah-langkah, lihat M emodifikasi kebijakan kepercayaan peran.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
```

```
    }
  ]
}
```

Memecahkan masalah kesalahan izin peran IAM

Saat mengaktifkan Perlindungan Malware untuk S3, GuardDuty periksa apakah peran layanan IAM Anda memiliki izin yang diperlukan untuk memvalidasi kepemilikan bucket Amazon S3. Jika izin ini hilang atau tidak dikonfigurasi dengan benar, Anda mungkin mendapatkan pesan berikut:

```
"message": "The request was rejected because provided IAM role does not have the
 required permissions to validate S3 bucket ownership."
"type": "InvalidInputException"
```

Skenario berikut dapat membantu Anda memecahkan masalah kesalahan ini:

Izin peran IAM tidak ada

- Peran IAM harus memiliki izin yang diperlukan untuk memungkinkan Perlindungan Malware untuk S3 untuk mengambil peran tersebut.
- GuardDuty memvalidasi kepemilikan bucket dengan `"s3:ListBucket"` izin. Ini harus ada dalam peran IAM yang Anda gunakan.

  Untuk informasi tentang izin, lihatMembuat atau memperbarui kebijakan peran IAM.

Ketersediaan peran IAM

- Saat Anda membuat peran IAM baru, biarkan beberapa menit agar perubahan mencapai konsistensi akhirnya sebelum mengaktifkan Perlindungan Malware untuk S3. Jika Anda mencoba mengaktifkan rencana perlindungan segera setelah membuat peran, validasi mungkin gagal.
- Untuk penyebaran Infrastructure as Code (IAc), GuardDuty merekomendasikan untuk mendeklarasikan ketergantungan sumber daya untuk memastikan peran IAM mencapai konsistensi akhirnya.

  Untuk contoh templat tentang cara melakukannya, lihat GuardDuty GitHubrepositori.

Cross-region pemberdayaan

Pastikan bucket Amazon S3 Anda berada di Wilayah yang sama tempat Anda mengaktifkan Perlindungan Malware untuk S3. GuardDuty

Langkah-langkah setelah mengaktifkan Perlindungan Malware untuk S3

Bagian ini mencantumkan langkah-langkah yang mungkin Anda ambil setelah mengaktifkan Perlindungan Malware untuk S3 untuk ember. Langkah-langkah berikut tercantum dalam urutan yang akan membantu Anda menavigasi langkah-langkah selanjutnya:

Untuk mengikuti setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda

1. Tambahkan kebijakan sumber daya kontrol akses berbasis tag (TBAC) — Saat Anda mengaktifkan penandaan, sebelum objek diunggah ke bucket yang dipilih, pastikan untuk menambahkan kebijakan TBAC ke sumber daya bucket S3 Anda. Untuk informasi selengkapnya, lihat Menambahkan TBAC pada sumber daya bucket S3.
2. Pantau status paket Perlindungan Malware — Pantau kolom Status untuk setiap bucket yang dilindungi. Untuk informasi tentang status potensial dan apa artinya, lihatMelihat dan memahami status bucket yang dilindungi.
3. Mulai pemindaian dengan memilih salah satu opsi berikut:
   - Unggah objek:
     1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
     2. Unggah file ke bucket S3 atau awalan objek yang Anda aktifkan fitur ini. Untuk langkah-langkah mengunggah file, lihat Mengunggah objek ke bucket Anda di Panduan Pengguna Amazon S3.
   - Memulai pemindaian sesuai permintaan: On-demand Pemindaian malware S3 masuk GuardDuty
4. Pantau status pemindaian objek S3 dan hasil pemindaian — Langkah ini mencakup informasi tentang cara memeriksa status pemindaian malware objek S3.

Diaktifkan keduanya GuardDuty dan Perlindungan Malware untuk S3	Perlindungan Malware yang Diaktifkan hanya untuk S3
• Ketika GuardDuty diaktifkan, itu dapat menghasilkan Perlindungan Malware untuk tipe pencarian S3 untuk menunjukkan keberadaan malware di objek S3 yang dipindai.	Anda berpotensi dapat memeriksa hasil pemindaian objek S3 dengan menggunakan satu atau beberapa opsi di bawahMemantau pemindaian objek S3 di Perlindungan Malware untuk S3. Ini termasuk menggunak

Diaktifkan keduanya GuardDuty dan Perlindungan Malware untuk S3	Perlindungan Malware yang Diaktifkan hanya untuk S3
• Anda berpotensi dapat memeriksa hasil pemindaian objek S3 dengan menggunakan satu atau beberapa opsi di bawahMemantau pemindaian objek S3 di Perlindungan Malware untuk S3. Ini termasuk menggunakan Amazon EventBridge, CloudWatch metrik untuk paket Perlindungan Malware, dan menandai objek yang dipindai.	an Amazon EventBridge, CloudWatch metrik untuk paket Perlindungan Malware, dan menandai objek yang dipindai.

On-demand Pemindaian malware S3 masuk GuardDuty

GuardDuty Perlindungan Malware untuk S3 terus memantau unggahan S3 baru. Untuk objek yang ada sebelum mengaktifkan perlindungan, atau untuk memindai ulang objek yang dipindai sebelumnya, Anda dapat memulai pemindaian malware S3 sesuai permintaan setelah Anda mengaktifkan paket Perlindungan GuardDuty Malware untuk bucket Anda.

On-demand Pemindaian malware menggunakan peran IAM Rencana Perlindungan Malware untuk akses objek dan menerapkan konfigurasi. Pemindaian akan mengganti awalan apa pun yang dikonfigurasi dalam Rencana Perlindungan Malware untuk bucket.

> **Note**
>
> Perlindungan Malware untuk kuota S3 berlaku untuk pemindaian malware sesuai permintaan. Untuk informasi lebih lanjut, LihatKuota dalam Perlindungan Malware untuk S3.
> Untuk informasi lebih lanjut tentang harga, lihatHarga dan biaya penggunaan untuk Perlindungan Malware untuk S3.

Prasyarat

Sebelum Anda memulai pemindaian malware sesuai permintaan, akun Anda harus memenuhi prasyarat berikut:

- Perlindungan Malware untuk S3 diaktifkan pada bucket target. Untuk informasi selengkapnya, lihat Mengkonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda.
- AWS kebijakan yang dikelola: AmazonGuardDutyFullAccess_v2 (direkomendasikan)Kebijakan ini dilampirkan ke pengguna IAM atau peran IAM yang menjalankan API.

Mulai pemindaian malware sesuai permintaan

Gunakan operasi SendObjectMalwareScanAPI, yang memerlukan jalur objek S3 sebagai input.

API/CLI

Anda dapat memindai versi terbaru dari objek atau menentukan versi tertentu untuk dipindai.

Untuk memindai versi tertentu dari suatu objek:

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket":
 "amzn-s3-demo-bucket", "Key": "APKAEIBAERJR2EXAMPLE", "VersionId":
 "d41d8cd98f00b204e9800998eEXAMPLE"}'
```

Untuk memindai versi terbaru dari suatu objek:

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket": "amzn-s3-demo-
bucket", "Key": "APKAEIBAERJR2EXAMPLE"}'
```

> **Important**
>
> Panggilan API yang berhasil mengonfirmasi bahwa permintaan pemindaian telah diterima. Namun, penting untuk memantau hasil pemindaian untuk memastikan penyelesaian yang berhasil dan untuk mengidentifikasi masalah apa pun, seperti kesalahan mengakses objek. Lihat informasi yang lebih lengkap di Memantau pemindaian objek S3 di Perlindungan Malware untuk S3.

Menggunakan kontrol akses berbasis tag (TBAC) dengan Perlindungan Malware untuk S3

Saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda, Anda dapat memilih untuk mengaktifkan penandaan. Setelah mencoba memindai objek S3 yang baru diunggah di bucket yang dipilih, GuardDuty tambahkan tag ke objek yang dipindai untuk memberikan status pemindaian malware. Ada biaya penggunaan langsung yang terkait saat Anda mengaktifkan penandaan. Untuk informasi selengkapnya, lihat Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3.

GuardDuty menggunakan tag yang telah ditentukan dengan kunci sebagai `GuardDutyMalwareScanStatus` dan nilai sebagai salah satu status pemindaian malware. Untuk informasi tentang nilai-nilai ini, lihatthe section called “Status pemindaian potensial objek S3 dan status hasil”.

Pertimbangan GuardDuty untuk menambahkan tag ke objek S3 Anda:

- Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek. Untuk informasi selengkapnya, lihat Mengkategorikan penyimpanan menggunakan tag di Panduan Pengguna Amazon S3.

  Jika semua 10 tag sudah digunakan, tidak GuardDuty dapat menambahkan tag yang telah ditentukan ke objek yang dipindai. GuardDuty juga menerbitkan hasil pemindaian ke bus EventBridge acara default Anda. Untuk informasi selengkapnya, lihat Memantau pemindaian objek S3 dengan Amazon EventBridge.
- Jika peran IAM yang dipilih tidak menyertakan izin GuardDuty untuk menandai objek S3, bahkan dengan penandaan diaktifkan untuk bucket Anda yang dilindungi, tidak GuardDuty akan dapat menambahkan tag ke objek S3 yang dipindai ini. Untuk informasi selengkapnya tentang izin peran IAM yang diperlukan untuk penandaan, lihat. Membuat atau memperbarui kebijakan peran IAM

  GuardDuty juga menerbitkan hasil pemindaian ke bus EventBridge acara default Anda. Untuk informasi selengkapnya, lihat Memantau pemindaian objek S3 dengan Amazon EventBridge.

Menambahkan TBAC pada sumber daya bucket S3

Anda dapat menggunakan kebijakan sumber daya bucket S3 untuk mengelola kontrol akses berbasis tag (TBAC) untuk objek S3 Anda. Anda dapat memberikan akses ke pengguna tertentu untuk mengakses dan membaca objek S3. Jika Anda memiliki organisasi yang dibuat dengan

menggunakan AWS Organizations, Anda harus menegakkan bahwa tidak ada yang dapat memodifikasi tag yang ditambahkan oleh GuardDuty. Untuk informasi selengkapnya, lihat Mencegah tag diubah kecuali oleh prinsipal resmi di Panduan Pengguna.AWS Organizations Contoh yang digunakan dalam topik terkait menyebutkan. `ec2` Saat Anda menggunakan contoh ini, ganti *`ec2`* dengan`s3`.

Daftar berikut menjelaskan apa yang dapat Anda lakukan dengan menggunakan TBAC:

- Cegah semua pengguna kecuali Perlindungan Malware untuk prinsipal layanan S3 membaca objek S3 yang belum ditandai dengan pasangan nilai kunci tag berikut:

  `GuardDutyMalwareScanStatus`:*`Potential key value`*
- Izinkan hanya GuardDuty untuk menambahkan kunci tag `GuardDutyMalwareScanStatus` dengan nilai sebagai hasil pemindaian, ke objek S3 yang dipindai. Templat kebijakan berikut dapat mengizinkan pengguna tertentu yang memiliki akses, untuk berpotensi mengganti pasangan nilai kunci tag.

Contoh kebijakan sumber daya bucket S3:

Ganti nilai placeholder berikut dalam kebijakan contoh:

- *`IAM-role-name`*- Berikan peran IAM yang Anda gunakan untuk mengonfigurasi Perlindungan Malware untuk S3 di bucket Anda.
- *`555555555555`*- Berikan yang Akun AWS terkait dengan ember yang dilindungi.
- *`amzn-s3-demo-bucket`*- Berikan nama bucket yang dilindungi.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "NoReadUnlessClean",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
                "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
                "arn:aws:iam::555555555555:role/IAM-role-name"
```

```
                ]
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:ExistingObjectTag/GuardDutyMalwareScanStatus":
 "NO_THREATS_FOUND"
                }
            }
        },
        {
            "Sid": "OnlyGuardDutyCanTagScanStatus",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
                    "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
                    "arn:aws:iam::555555555555:role/IAM-role-name"
                ]
            },
            "Action": "s3:PutObjectTagging",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "s3:RequestObjectTagKeys": "GuardDutyMalwareScanStatus"
                }
            }
        }
    ]
}
```

Untuk informasi selengkapnya tentang menandai sumber daya S3 Anda, kebijakan Penandaan dan kontrol akses.

Melihat dan memahami status bucket yang dilindungi

Setelah mengaktifkan Perlindungan Malware untuk S3 untuk bucket, status menunjukkan apakah fitur tersebut dikonfigurasi dan berfungsi seperti yang diharapkan. Status ini dikaitkan dengan pengenal paket Perlindungan Malware (ID) yang unik. GuardDuty membuat ID ini pada saat mengaktifkan fitur.

Gunakan prosedur berikut untuk melihat status bucket yang dilindungi:

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Perlindungan Malware untuk S3.
3. Di tabel bucket Protected, lihat kolom Status yang sesuai untuk bucket S3 Anda.

Tabel berikut mencantumkan dan menjelaskan nilai status yang terkait dengan sumber daya paket Perlindungan Malware Anda. Dengan memahami apa arti status ini bagi bucket yang dilindungi, Anda dapat memastikan bahwa GuardDuty memulai pemindaian malware otomatis saat objek diunggah.

Status	Deskripsi
Aktif	Bucket S3 Anda telah berhasil dikonfigurasi dengan Perlindungan Malware untuk S3. Saat status Aktif, perubahan pada peran IAM (penghapusan atau modifikasi izin) tidak akan memperbarui status ke Peringatan atau Kesalahan. Kami merekomendasikan untuk memantau status pemindaian secara terus menerus dengan menggunakan salah satu metode yang dijelaskan dalamMemantau pemindaian objek S3.
Peringatan *	Perlindungan Malware untuk S3 dirancang agar tidak terpengaruh saat peringatan muncul. Ketika GuardDuty melihat objek S3 baru, itu akan memulai pemindaian malware. Setelah berhasil memulai pemindaian, nilai kolom Status mungkin memerlukan beberapa menit untuk berubah menjadi Aktif. Anda akan menerima EventBridge pemberitahuan setelah pembaruan nilai kolom Status.

Status	Deskripsi
Kesalahan [*] -	Ember Anda tidak terlindungi. Tak satu pun dari pemindaian malware yang terkait dengan bucket S3 ini akan selesai. Mungkin ada satu atau lebih akar penyebab potensial.

[*] Untuk informasi tentang potensi masalah dan langkah-langkah terkait untuk menyelesaikannya, lihatMemecahkan masalah status paket Perlindungan Malware.

Memantau pemindaian objek S3 di Perlindungan Malware untuk S3

Saat menggunakan Perlindungan Malware untuk S3 dengan ID GuardDuty detektor, jika objek Amazon S3 Anda berpotensi berbahaya GuardDuty , akan dihasilkan. Perlindungan Malware untuk tipe pencarian S3 Menggunakan GuardDuty konsol dan API, Anda dapat melihat temuan yang dihasilkan. Untuk informasi tentang memahami jenis temuan ini, lihatDetail temuan.

Saat menggunakan Perlindungan Malware untuk S3 tanpa mengaktifkan GuardDuty (tanpa ID detektor), bahkan ketika objek Amazon S3 yang dipindai berpotensi berbahaya, tidak GuardDuty dapat menghasilkan temuan apa pun.

Daftar Isi

- Status pemindaian potensial objek S3 dan status hasil
- Memantau pemindaian objek S3 dengan Amazon EventBridge
- Memantau pemindaian objek S3 dengan GuardDuty tag terkelola
- Metrik status pemindaian objek S3 di CloudWatch

Status pemindaian potensial objek S3 dan status hasil

Bagian ini menjelaskan potensi nilai status pemindaian objek S3 dan nilai hasil pemindaian.

Status pemindaian objek S3 menunjukkan status pemindaian malware, seperti selesai, dilewati, atau gagal.

Status hasil pemindaian malware objek S3 menunjukkan hasil pemindaian berdasarkan nilai status pemindaian. Setiap nilai status hasil pemindaian malware memetakan ke status pemindaian.

Daftar berikut memberikan nilai hasil pemindaian objek S3 potensial. Jika Anda telah mengaktifkan penandaan, Anda dapat memantau hasil pemindaian dengan Menggunakan Tag Objek S3. Setelah pemindaian, nilai tag akan memiliki salah satu nilai hasil pemindaian berikut.

Nilai status hasil pemindaian malware potensial objek S3

- `NO_THREATS_FOUND` — GuardDuty mendeteksi tidak ada ancaman potensial yang terkait dengan objek yang dipindai.
- `THREATS_FOUND` — GuardDuty mendeteksi potensi ancaman yang terkait dengan objek yang dipindai.
- `UNSUPPORTED` — Ada beberapa alasan mengapa Perlindungan Malware untuk S3 akan melewatkan pemindaian. Alasan potensial termasuk file yang dilindungi kata sandi, arsip dengan rasio kompresi yang sangat tinggi Perlindungan Malware untuk kuota S3, dan dukungan untuk fitur Amazon S3 tertentu mungkin tidak tersedia. Untuk informasi selengkapnya, lihat Kemampuan Perlindungan Malware untuk S3.
- `ACCESS_DENIED` — tidak GuardDuty dapat mengakses objek ini untuk pemindaian. Periksa izin peran IAM yang terkait dengan bucket ini. Untuk informasi selengkapnya, lihat Membuat atau memperbarui kebijakan peran IAM.

  Jika Anda telah mengaktifkan penandaan objek S3 pasca-pemindaian, lihat. Memecahkan masalah kegagalan tag pasca-pemindaian objek S3
- `FAILED` — tidak GuardDuty dapat melakukan pemindaian malware pada objek ini karena kesalahan internal.

Daftar berikut memberikan nilai status pemindaian objek S3 potensial dan pemetaannya ke hasil pemindaian objek S3.

Nilai status pemindaian potensial objek S3

- Selesai — Pemindaian berhasil diselesaikan dan menunjukkan apakah objek S3 memiliki malware. Dalam hal ini, potensi nilai hasil pemindaian objek S3 dapat berupa `THREATS_FOUND` atau `NO_THREATS_FOUND`.
- Dilewati — GuardDuty melewatkan pemindaian malware saat memindai objek S3 ini tidak didukung oleh Perlindungan Malware untuk S3, atau GuardDuty tidak memiliki akses ke objek S3 yang diunggah di bucket yang dipilih.

Dalam hal ini, potensi nilai hasil pemindaian objek S3 dapat berupa `UNSUPPORTED` atau`ACCESS_DENIED`.

GuardDuty juga akan melewatkan pemindaian jika peran IAM yang diperlukan dihapus.

- Gagal — Mirip dengan nilai hasil pemindaian objek S3`FAILED`, status pemindaian GuardDuty ini berarti tidak dapat melakukan pemindaian malware pada objek S3 karena kesalahan internal.

Saat status pemindaian`SKIPPED`, EventBridge pemberitahuan untuk hasil pemindaian objek S3 menyertakan `statusReasons` bidang di dalamnya`scanResultDetails`. Bidang ini adalah daftar string yang memberikan alasan spesifik mengapa pemindaian dilewati. Tabel berikut menjelaskan `statusReasons` nilai yang mungkin.

Alasan status	Pindai status hasil	Deskripsi
`UNAUTHORIZED_TO_GET_OBJECT`	`ACCESS_DENIED`	Perlindungan Malware untuk S3 tidak memiliki izin untuk membaca objek S3, atau objek S3 tidak ada. Verifikasi bahwa peran IAM yang terkait dengan bucket yang dilindungi memiliki izin yang diperlukan dan AWS KMS kebijakan bucket apa pun memungkinkan peran tersebut untuk mendekripsi objek.
`UNAUTHORIZED_TO_ASSUME_ROLE`	`ACCESS_DENIED`	Perlindungan Malware untuk S3 tidak dapat mengasumsikan peran IAM yang dikonfigurasi untuk bucket yang dilindungi. Verifikasi bahwa kebijakan kepercayaan peran memungkin kan Perlindungan Malware untuk S3 untuk mengambil peran.
`SSE_C_ENCRYPTED_OBJECT`	`ACCESS_DENIED`	Objek S3 dienkripsi dengan kunci enkripsi yang disediakan pelanggan (). SSE-C GuardDuty tidak dapat mengakses objek yang dienkripsi dengan. SSE-C Untuk informasi selengkapnya, lihat Dukungan fitur Amazon S3.

Alasan status	Pindai status hasil	Deskripsi
OBJECT_E_TAG_CHANGED	ACCESS_DENIED	Objek S3 ETag berubah antara waktu pemindaian dimulai dan ketika GuardDuty mencoba membaca objek. Unggahan berikutnya atau versi baru akan dipindai.
BUCKET_NOT_FOUND	ACCESS_DENIED	Bucket S3 yang terkait dengan pemindaian tidak ada lagi.
UNSUPPORTED_STORAGE_CLASS	UNSUPPORTED	Objek S3 menggunakan kelas penyimpanan yang tidak didukung oleh Perlindungan Malware untuk S3. Untuk informasi selengkapnya, lihat Dukungan fitur Amazon S3.
OBJECT_SIZE_LIMIT_EXCEEDED	UNSUPPORTED	Ukuran objek S3 melebihi batas ukuran file maksimum untuk Perlindungan Malware untuk S3. Untuk informasi selengkapnya, lihat Perlindungan Malware untuk kuota S3.
PASSWORD_PROTECTED	UNSUPPORTED	Objek dilindungi kata sandi.
EXTRACTED_FILE_LIMIT_EXCEEDED	UNSUPPORTED	Arsip berisi lebih banyak file dari batas maksimum yang diizinkan. Untuk informasi selengkapnya, lihat Perlindungan Malware untuk kuota S3.
EXTRACTED_LEVEL_LIMIT_EXCEEDED	UNSUPPORTED	Arsip melebihi kedalaman bersarang maksimum yang diizinkan.
EXTRACTED_BYTE_LIMIT_EXCEEDED	UNSUPPORTED	Konten arsip yang diekstraksi melebihi ukuran byte maksimum yang diizinkan. Untuk informasi selengkapnya, lihat Perlindungan Malware untuk kuota S3.

Alasan status	Pindai status hasil	Deskripsi
`EXTRACTION_RATIO_LIMIT_EXCEEDED`	`UNSUPPORTED`	Arsip memiliki rasio kompresi yang sangat tinggi yang melebihi batas yang diizinkan. Untuk informasi selengkapnya, lihat Perlindungan Malware untuk kuota S3.

Memantau pemindaian objek S3 dengan Amazon EventBridge

Amazon EventBridge adalah layanan bus acara tanpa server yang memudahkan untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. EventBridge mengirimkan aliran data real-time dari aplikasi Anda sendiri, aplikasi Software-as-a-Service (SaaS), AWS dan layanan serta rute data tersebut ke target seperti Lambda. Hal ini memungkinkan Anda memantau kejadian yang terjadi dalam layanan, dan membangun arsitektur yang didorong kejadian. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

Sebagai akun pemilik bucket S3 yang dilindungi dengan Perlindungan Malware untuk S3, GuardDuty menerbitkan EventBridge notifikasi ke bus acara default dalam skenario berikut:

- Perubahan status sumber daya paket Perlindungan Malware untuk setiap bucket Anda yang dilindungi. Untuk informasi tentang berbagai status, lihatMelihat dan memahami status bucket yang dilindungi.

  Untuk menyiapkan aturan Amazon EventBridge (EventBridge) untuk status sumber daya, lihatStatus sumber daya paket Perlindungan Malware.
- Hasil pemindaian objek S3 akan dipublikasikan ke bus EventBridge acara default Anda.

  `s3Throttled`Bidang menunjukkan apakah ada penundaan dalam mengunggah atau mengambil penyimpanan dari Amazon S3 atau tidak. Nilai `true` menunjukkan bahwa ada penundaan, dan `false` menunjukkan bahwa tidak ada penundaan.

  Jika `s3Throttled` `true` untuk hasil pemindaian Anda, Amazon S3 merekomendasikan pengaturan awalan dengan cara yang membantu Anda mengurangi transaksi per detik (TPS) untuk setiap awalan. Untuk informasi selengkapnya, lihat Pola desain praktik terbaik: mengoptimalkan kinerja Amazon S3 di Panduan Pengguna Amazon S3.

Untuk menyiapkan aturan Amazon EventBridge (EventBridge) untuk hasil pemindaian objek S3, lihatHasil pemindaian objek S3.

- Ada peristiwa kegagalan tag pasca-pemindaian karena alasan berikut:
  - Peran IAM Anda tidak memiliki izin untuk menandai objek.

    Menambahkan izin kebijakan IAMTemplate termasuk izin GuardDuty untuk menandai objek.
  - Sumber daya bucket atau objek yang ditentukan dalam peran IAM tidak ada lagi.
  - Objek S3 terkait telah mencapai batas tag maksimum. Untuk informasi selengkapnya tentang batas tag, lihat Mengkategorikan penyimpanan menggunakan tag di Panduan Pengguna Amazon S3.

  Untuk menyiapkan aturan Amazon EventBridge (EventBridge) untuk peristiwa kegagalan tag pasca-pemindaian, lihatPost-scan menandai peristiwa kegagalan.

Menyiapkan EventBridge aturan

Anda dapat mengatur EventBridge aturan di akun Anda untuk mengirim status sumber daya, peristiwa kegagalan tag pasca-pemindaian, atau hasil pemindaian objek S3 ke yang lain. Layanan AWS Sebagai akun GuardDuty administrator yang didelegasikan, Anda akan menerima pemberitahuan status sumber daya paket Perlindungan Malware ketika ada perubahan status.

EventBridge Harga standar akan berlaku. Untuk informasi selengkapnya, lihat EventBridge harga Amazon.

Semua nilai yang muncul di *red* adalah placeholder untuk contoh. Nilai-nilai ini akan berubah berdasarkan nilai di akun Anda, dan apakah malware terdeteksi atau tidak.

Topik

- Status sumber daya paket Perlindungan Malware
- Hasil pemindaian objek S3
- Post-scan menandai peristiwa kegagalan

Status sumber daya paket Perlindungan Malware

Anda dapat membuat pola EventBridge acara berdasarkan skenario berikut:

Nilai **`tipe detail`** potensial

- `"GuardDuty Malware Protection Resource Status Active"`
- `"GuardDuty Malware Protection Resource Status Warning"`
- `"GuardDuty Malware Protection Resource Status Error"`

Pola acara

```
{
      "detail-type": ["potential detail-type"],
      "source": ["aws.guardduty"]
}
```

Skema pemberitahuan sampel untuk **`GuardDuty Malware Protection Resource Status Active`**:

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "GuardDuty Malware Protection Resource Status Active",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "ACTIVE"
    }
}
```

Skema pemberitahuan sampel untuk **`GuardDuty Malware Protection Resource Status Warning`**:

```
{
```

```
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "GuardDuty Malware Protection Resource Status warning",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "WARNING",
        "statusReasons": [
         {
            "code": "INSUFFICIENT_TEST_OBJECT_PERMISSIONS"
         }
        ]
    }
}
```

Skema pemberitahuan sampel untuk **`GuardDuty Malware Protection Resource Status Error`**:

```
{
    "version": "0",
    "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
    "detail-type": "GuardDuty Malware Protection Resource Status Error",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
```

```
        "resourceStatus": "ERROR",
        "statusReasons": [
        {
            "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
        }
       ]
    }
}
```

Berdasarkan alasan di balik `resourceStatus`ERROR, `statusReasons` nilainya akan terisi.

Untuk informasi tentang langkah-langkah pemecahan masalah untuk peringatan dan kesalahan berikut, lihat. Memecahkan masalah status paket Perlindungan Malware

Hasil pemindaian objek S3

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}
```

Ketika `scanStatus` ituSKIPPED, `scanResultDetails` termasuk `statusReasons` bidang yang memberikan alasan spesifik mengapa pemindaian dilewati. Untuk informasi tentang nilai yang mungkin, lihatStatus pemindaian potensial objek S3 dan status hasil.

Skema pemberitahuan sampel untuk **`NO_THREATS_FOUND`**:

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
```

```
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "NO_THREATS_FOUND",
            "threats": null,
            "statusReasons": null
        }
    }
}
```

Skema pemberitahuan sampel untuk **THREATS_FOUND**:

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "THREATS_FOUND",
            "threats": [
                {
                    "name": "EICAR-Test-File (not a virus)",
                    "source": "AMAZON",
```

```
                    "itemDetails": [{
                        "hash":
 "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
                        "itemPath": "APKAEIBAERJR2EXAMPLE"
                    }]
                }
            ],
            "statusReasons": null
        }
    }
}
```

> **Note**
>
> `scanResultDetails.Threats`Bidang ini hanya berisi satu ancaman. Secara default, Perlindungan Malware untuk pemindaian S3 melaporkan ancaman pertama yang terdeteksi. Setelah ini, `scanStatus` diatur ke`COMPLETED`.

Skema pemberitahuan sampel untuk status hasil pemindaian **`UNSUPPORTED`** (Dilewati):

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
```

```
        "scanResultDetails": {
            "scanResultStatus": "UNSUPPORTED",
            "threats": null,
            "statusReasons": ["PASSWORD_PROTECTED"]
        }
    }
}
```

Skema pemberitahuan sampel untuk status hasil pemindaian **`ACCESS_DENIED`** (Dilewati):

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "ACCESS_DENIED",
            "threats": null,
            "statusReasons": ["SSE_C_ENCRYPTED_OBJECT"]
        }
    }
}
```

Skema pemberitahuan sampel untuk status **`FAILED`** hasil pemindaian:

```
{
    "version": "0",
```

```
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "FAILED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "FAILED",
            "threats": null,
            "statusReasons": null
        }
    }
}
```

Post-scan menandai peristiwa kegagalan

Pola acara:

```
{
      "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
      "source": "aws.guardduty"
 }
```

Skema pemberitahuan sampel untuk **`ACCESS_DENIED`**:

```
{
    "version": "0",
    "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
    "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
    "source": "aws.guardduty",
```

```
    "account": "111122223333",
    "time": "2024-06-10T16:16:08Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-06-10T16:16:08Z",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "failureReason": "ACCESS_DENIED"
        }]
    }
}
```

Skema pemberitahuan sampel untuk **`MAX_TAG_LIMIT_EXCEEDED`**:

```
{
    "version": "0",
    "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
    "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-06-10T16:16:08Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-06-10T16:16:08Z",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
```

```
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "failureReason": "MAX_TAG_LIMIT_EXCEEDED"
        }]
    }
}
```

Untuk memecahkan masalah alasan kegagalan ini, lihat. Memecahkan masalah kegagalan tag pasca-pemindaian objek S3

Memantau pemindaian objek S3 dengan GuardDuty tag terkelola

Gunakan opsi aktifkan penandaan sehingga GuardDuty dapat menambahkan tag ke objek Amazon S3 Anda setelah menyelesaikan pemindaian malware.

Pertimbangan untuk mengaktifkan penandaan

- Ada biaya penggunaan terkait saat GuardDuty menandai objek S3 Anda. Untuk informasi selengkapnya, lihat Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3.
- Anda harus menyimpan izin penandaan yang diperlukan untuk peran IAM pilihan yang terkait dengan bucket ini; jika tidak, tidak GuardDuty dapat menambahkan tag ke objek yang dipindai. Peran IAM sudah menyertakan izin untuk menambahkan tag ke objek S3 yang dipindai. Untuk informasi selengkapnya, lihat Membuat atau memperbarui kebijakan peran IAM.
- Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek S3. Untuk informasi selengkapnya, lihat Menggunakan kontrol akses berbasis tag (TBAC).

Setelah Anda mengaktifkan penandaan untuk bucket S3 atau awalan tertentu, objek apa pun yang baru diunggah yang dipindai, akan memiliki tag terkait dalam format pasangan nilai kunci berikut:

`GuardDutyMalwareScanStatus`:*`Scan-Result-Status`*

Untuk informasi tentang nilai tag potensial, lihatStatus pemindaian potensial objek S3 dan status hasil.

Memecahkan masalah kegagalan tag pasca-pemindaian objek S3 di Perlindungan Malware untuk S3

Bagian ini hanya berlaku untuk Anda jika Anda Aktifkan penandaan untuk objek yang dipindai berada dalam ember yang dilindungi.

Saat GuardDuty mencoba menambahkan tag ke objek S3 yang dipindai, tindakan penandaan dapat mengakibatkan kegagalan. Alasan potensial mengapa hal ini dapat terjadi pada ember Anda adalah `ACCESS_DENIED` dan`MAX_TAG_LIMIT_EXCEEDED`. Gunakan topik berikut untuk memahami alasan potensial untuk alasan kegagalan tag pasca-pemindaian ini dan selesaikan masalahnya.

ACCESS_DITOLAK

Daftar berikut memberikan alasan potensial yang dapat menyebabkan masalah ini:

- Peran IAM yang digunakan untuk bucket S3 yang dilindungi ini tidak memiliki izin. AllowPostScanTag Verifikasi bahwa peran IAM terkait menggunakan kebijakan bucket ini. Untuk informasi selengkapnya, lihat Membuat atau memperbarui kebijakan peran IAM.
- Kebijakan bucket S3 yang dilindungi tidak memungkinkan GuardDuty untuk menambahkan tag ke objek ini.
- Objek S3 yang dipindai tidak ada lagi.

MAX_TAG_LIMIT_EXCEEDED

Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek S3. Untuk informasi selengkapnya, lihat Pertimbangan GuardDuty untuk menambahkan tag ke objek S3 Anda di bawah. Aktifkan penandaan untuk objek yang dipindai

Metrik status pemindaian objek S3 di CloudWatch

Anda dapat memantau GuardDuty penggunaan CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati waktu nyata. Statistik ini disimpan selama 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang bagaimana kinerja Perlindungan Malware untuk S3. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

CloudWatch Metrik untuk Perlindungan Malware untuk S3 tersedia di tingkat sumber daya. Anda dapat menanyakan metrik ini untuk setiap sumber daya yang dilindungi secara terpisah. Metrik dilaporkan di `AWS/GuardDuty/MalwareProtection` namespace. Anda dapat mengatur alarm pada sumber daya tertentu untuk memantau postur keamanan.

Metrik status pemindaian malware

Metrik	Deskripsi
`CompletedScanCount`	Jumlah pemindaian malware objek S3 yang diselesaikan dalam jangka waktu tertentu. Dimensi yang Valid: • `Malware Protection Plan Id` `Resource Name` Unit: Hitungan
`FailedScanCount`	Jumlah pemindaian malware objek S3 yang gagal dalam jangka waktu tertentu. Dimensi yang Valid: • `Malware Protection Plan Id` `Resource Name` Unit: Hitungan

`SkippedScanCount`	Jumlah pemindaian malware objek S3 yang dilewati dalam jangka waktu tertentu.
	
	Dimensi yang Valid:
	
	• `Malware Protection Plan Id`
	
	`Resource Name`
	
	`Skipped Reason`
	
	Nilai potensial
	
	• `Unsupported`
	• `MissingPermissions`
	
	Unit: Hitungan

Metrik hasil pemindaian malware	
`InfectedScanCount`	Jumlah pemindaian malware objek S3 yang mendeteksi objek yang berpotensi berbahaya dalam jangka waktu tertentu. Dimensi yang Valid: • `Malware Protection Plan Id` `Resource Name` Unit: Hitungan

`CompletedScanBytes`	Jumlah byte objek S3 yang dipindai dalam kerangka waktu tertentu. Dimensi yang Valid: • `Malware Protection Plan Id` `Resource Name` Unit: Hitungan

> **Note**
>
> Secara default, statistik dalam CloudWatch metrik adalah AVG.

Dimensi berikut didukung untuk metrik Perlindungan Malware untuk S3.

Dimensi	Deskripsi
`Malware Protection Plan Id`	Pengidentifikasi unik yang terkait dengan sumber daya paket Perlindungan Malware yang GuardDuty dibuat untuk sumber daya Anda yang dilindungi.
`Resource Name`	Nama sumber daya yang dilindungi.
`Skipped Reason`	Alasan mengapa pemindaian malware objek S3 dilewati. Nilai potensial • `Unsupported` • `MissingPermissions`

Untuk informasi tentang mengakses dan menanyakan metrik ini, lihat Menggunakan metrik Amazon CloudWatch di Panduan Pengguna Amazon. CloudWatch

Untuk informasi tentang mengatur alarm, lihat Menggunakan CloudWatch alarm Amazon di CloudWatch Panduan Pengguna Amazon.

Pemecahan Masalah

Konten

- Memecahkan masalah status paket Perlindungan Malware
- Memecahkan masalah pemindaian malware sesuai permintaan

Memecahkan masalah status paket Perlindungan Malware

Untuk bucket yang dilindungi, GuardDuty menampilkan Status berdasarkan peringkat. Misalnya, jika bucket yang dilindungi memiliki masalah di kategori Kesalahan dan Peringatan, pertama-tama GuardDuty akan menampilkan masalah yang terkait dengan status Kesalahan.

Daftar berikut mencakup kesalahan dan peringatan untuk status paket Perlindungan Malware.

Kesalahan

- EventBridge pemberitahuan dinonaktifkan untuk bucket S3 ini
- EventBridge aturan terkelola untuk menerima peristiwa bucket S3 tidak ada
- Bucket S3 tidak ada lagi

Peringatan

Tidak dapat menempatkan objek uji

EventBridge pemberitahuan dinonaktifkan untuk bucket S3 ini

Kode alasan status terkait adalah`EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED`.

Detail status

GuardDuty menggunakan EventBridge untuk menerima pemberitahuan saat objek baru diunggah ke bucket S3 ini. Izin ini tidak ada dalam peran IAM Anda.

Langkah-langkah untuk memecahkan masalah

Opsi 1: Tambahkan pernyataan izin berikut ke peran IAM Anda:

```
{
```

```
            "Sid": "AllowEnableS3EventBridgeEvents",
            "Effect": "Allow",
            "Action": [
               "s3:PutBucketNotification",
               "s3:GetBucketNotification"
               ],
            "Resource": [
               "arn:aws:s3:::amzn-s3-demo-bucket"
              ]
}
```

Ganti *amzn-s3-demo-bucket* dengan nama bucket Amazon S3 Anda.

Opsi 2: Aktifkan EventBridge notifikasi dengan menggunakan konsol Amazon S3

1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Pada halaman Bucket, di bawah tab Bucket tujuan umum, pilih nama bucket yang terkait dengan kesalahan ini.
3. Pada halaman bucket ini, pilih tab Properties.
4. Di bawah EventBridge bagian Amazon, pilih Edit.
5. Di EventBridge halaman Edit Amazon, untuk Kirim pemberitahuan ke Amazon EventBridge untuk semua acara di bucket ini, pilih Aktif.
6. Pilih Simpan perubahan.

Mungkin perlu beberapa menit agar nilai kolom Status berubah menjadi Aktif.

EventBridge aturan terkelola untuk menerima peristiwa bucket S3 tidak ada

Kode alasan status terkait adalah`EVENTBRIDGE_MANAGED_RULE_DISABLED`.

Detail status

EventBridge Izin aturan terkelola untuk mengelola pengaturan EventBridge aturan tidak ada.

Langkah-langkah untuk memecahkan masalah

Tambahkan pernyataan izin berikut ke peran IAM Anda:

```
{
```

```
          "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
         "Effect": "Allow",
         "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
         "Resource": [
            "arn:aws:events:*:*:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ],
         "Condition": {
            "StringEquals": {
               "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
               }
            }
}
```

Mungkin perlu beberapa menit agar nilai kolom Status berubah menjadi Aktif.

Bucket S3 tidak ada lagi

Kode alasan status terkait adalah`PROTECTED_RESOURCE_DELETED`.

Detail status

Bucket S3 ini telah dihapus dari akun Anda dan tidak ada lagi.

Langkah untuk memecahkan masalah

Jika menghapus bucket S3 tidak disengaja, maka Anda dapat membuat bucket baru dengan menggunakan konsol Amazon S3.

Setelah berhasil membuat bucket, aktifkan Perlindungan Malware untuk S3 dengan mengikuti langkah-langkah di bawah Mengkonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda halaman.

Tidak dapat menempatkan objek uji

Kode alasan status terkait adalah`INSUFFICIENT_TEST_OBJECT_PERMISSIONS`.

> **Note**
>
> Izin untuk menambahkan objek uji adalah opsional. Kehilangan izin ini dalam peran IAM Anda tidak mencegah Perlindungan Malware untuk S3 untuk memulai pemindaian malware pada objek yang baru diunggah. Setelah pemindaian berhasil dimulai, mungkin diperlukan beberapa menit agar Status paket Perlindungan Malware berubah dari Peringatan menjadi Aktif.
> Jika peran IAM sudah menyertakan izin ini, maka peringatan ini menunjukkan kebijakan bucket Amazon S3 terbatas yang tidak mengizinkan akses IAM untuk menempatkan objek pengujian di bucket S3 ini.

Detail status

Untuk memvalidasi penyiapan bucket yang dipilih, GuardDuty letakkan objek uji di bucket Anda.

Langkah-langkah untuk memecahkan masalah

Anda dapat memilih untuk memperbarui peran IAM untuk menyertakan izin yang hilang. Untuk peran IAM yang dipilih, tambahkan izin berikut sehingga GuardDuty dapat menempatkan objek uji ke sumber daya yang dipilih:

```
{
         "Sid": "AllowPutValidationObject",
         "Effect": "Allow",
         "Action": [
           "s3:PutObject"
           ],
         "Resource": [
           "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-
object"
           ]
}
```

Ganti *amzn-s3-demo-bucket* dengan nama bucket Amazon S3 Anda. Untuk informasi tentang izin peran IAM, lihat. Membuat atau memperbarui kebijakan peran IAM

Mungkin perlu beberapa menit agar nilai kolom Status berubah menjadi Aktif.

Memecahkan masalah pemindaian malware sesuai permintaan

Tidak dapat memulai pemindaian.

Pastikan permintaan pemindaian berisi masukan yang valid dan Rencana Perlindungan Malware diaktifkan untuk bucket.

Mengedit paket Perlindungan Malware untuk bucket yang dilindungi

Anda mungkin perlu mengedit kebijakan izin IAM yang disukai, mengaktifkan atau menonaktifkan penandaan objek S3 yang dipindai, atau menambah atau menghapus awalan objek S3. Misalnya, saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket, Anda memutuskan untuk tidak mengaktifkan penandaan objek S3 yang dipindai dengan hasil pemindaian. Namun, sekarang Anda GuardDuty ingin menambahkan tag yang telah ditentukan dan hasil pemindaian sebagai nilai tag.

Pilih metode akses pilihan untuk memperbarui paket Perlindungan Malware untuk bucket S3 Anda yang dilindungi.

Console

Untuk mengedit paket Perlindungan Malware

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Perlindungan Malware untuk S3.
3. Di dalam bucket Protected, pilih bucket yang ingin Anda edit konfigurasi yang ada.
4. Pilih Edit.
5. Perbarui konfigurasi dan pengaturan yang ada untuk bucket Anda dan konfirmasikan perubahannya. Untuk informasi tentang deskripsi dan langkah-langkah untuk setiap bagian, lihatMengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda.

   Pantau kolom Status untuk bucket yang dilindungi ini. Jika muncul sebagai Peringatan atau Kesalahan, lihatMemecahkan masalah status paket Perlindungan Malware.

API/CLI

Untuk mengedit paket Perlindungan Malware dengan menggunakan API atau AWS CLI

- Dengan menggunakan API

Jalankan UpdateMalwareProtectionPlanAPI dengan menggunakan ID paket Perlindungan Malware yang terkait dengan sumber daya paket ini.

Untuk mengambil ID paket Perlindungan Malware di Wilayah tertentu, Anda dapat menjalankan ListMalwareProtectionPlansAPI di Wilayah tersebut.

- Dengan menggunakan AWS CLI

  Daftar berikut memberikan AWS CLI contoh perintah untuk memperbarui sumber daya paket Perlindungan Malware. Anda akan memerlukan ID paket Perlindungan Malware yang terkait dengan bucket S3 Anda.

  AWS CLI contoh perintah

  - Gunakan AWS CLI perintah berikut untuk mengaktifkan atau menonaktifkan penandaan untuk sumber daya paket Perlindungan Malware yang terkait dengan bucket S3 Anda:

    ```
    aws guardduty update-malware-protection-plan --malware-protection-plan-
    id 4cc8bf26c4d75EXAMPLE --actions "Tagging"={"Status"="ENABLED|DISABLED"}
    ```

  - Gunakan AWS CLI perintah berikut untuk menambahkan awalan objek ke sumber daya paket Perlindungan Malware yang terkait dengan bucket S3 Anda:

    ```
    aws guardduty update-malware-protection-plan --malware-
    protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource
     "S3Bucket"={"ObjectPrefixes"=["amzn-s3-demo-1", "amzn-s3-demo-2"]}
    ```

    Pastikan untuk menyertakan awalan objek yang ada dalam perintah ini; jika tidak, GuardDuty akan menghapus awalan tersebut saat mengedit sumber daya paket Perlindungan Malware.

  - Gunakan AWS CLI perintah berikut untuk menghapus awalan objek dari sumber daya paket Perlindungan Malware yang terkait dengan bucket S3 Anda:

    ```
    aws guardduty update-malware-protection-plan --malware-protection-plan-
    id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=[""]}
    ```

  Jika Anda belum memiliki ID paket Perlindungan Malware untuk sumber daya ini, Anda dapat menjalankan AWS CLI perintah berikut dan menggantinya *us-east-1* dengan Wilayah yang ingin Anda cantumkan ID paket Perlindungan Malware.

```
aws guardduty list-malware-protection-plans --region us-east-1
```

Menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi

Saat Anda menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi, GuardDuty menghapus ID paket Perlindungan Malware yang terkait dengan bucket tersebut. GuardDuty tidak akan lagi memulai pemindaian malware ketika objek baru diunggah ke bucket ini atau salah satu awalan objek yang dipilih.

Jika Anda telah mengaktifkan GuardDuty dan sekarang ingin menangguhkan atau menonaktifkan GuardDuty, lihatMenangguhkan atau menonaktifkan GuardDuty. Karena tidak ada konsep ID detektor dalam Perlindungan Malware untuk S3, menonaktifkan atau menangguhkan GuardDuty tidak memengaruhi status bucket yang dilindungi di akun Anda. Anda dapat terus menggunakan fitur Perlindungan Malware untuk S3 secara independen dengan harga standar terkait. Untuk informasi selengkapnya, lihat Meninjau biaya penggunaan untuk Perlindungan Malware untuk S3. Untuk berhenti menggunakan Perlindungan Malware untuk S3, Anda harus menonaktifkannya untuk semua ember yang dilindungi di akun Anda. Jika Anda ingin terus menggunakan GuardDuty dan menonaktifkan hanya Perlindungan Malware untuk S3 untuk bucket, langkah-langkah berikut tidak akan memengaruhi konfigurasi GuardDuty layanan dan paket perlindungan lain yang mungkin telah Anda aktifkan.

Pilih metode akses pilihan untuk menonaktifkan Perlindungan Malware untuk S3 di bucket S3 Anda yang dilindungi.

Console

Untuk menonaktifkan Perlindungan Malware untuk S3 dengan menggunakan konsol GuardDuty

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Perlindungan Malware untuk S3.
3. Di dalam bucket Protected, pilih bucket yang ingin Anda nonaktifkan Perlindungan Malware untuk S3.

Anda hanya dapat memilih satu ember yang dilindungi sekaligus. Untuk menonaktifkan Perlindungan Malware untuk S3 selama lebih dari satu bucket, ikuti langkah-langkah ini lagi untuk bucket S3 lainnya.

4. Pilih Nonaktifkan untuk mengonfirmasi pilihan.

API/CLI

Untuk menonaktifkan Perlindungan Malware untuk S3 dengan menggunakan API atau AWS CLI

- Dengan menggunakan API

  Jalankan DeleteMalwareProtectionPlanAPI dengan menggunakan ID paket Perlindungan Malware yang terkait dengan sumber daya paket ini.

  Untuk mengambil ID paket Perlindungan Malware, Anda dapat menjalankan ListMalwareProtectionPlansAPI.

- Dengan menggunakan AWS CLI

  Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk menonaktifkan Perlindungan Malware untuk S3 *4cc8bf26c4d75EXAMPLE* dengan menggantinya dengan ID paket Perlindungan Malware yang terkait dengan bucket S3 ini:

```
aws guardduty delete-malware-protection-plan --malware-protection-plan-
id 4cc8bf26c4d75EXAMPLE
```

  Jika Anda belum memiliki ID paket Perlindungan Malware untuk bucket S3 ini, Anda dapat menjalankan AWS CLI perintah berikut dan menggantinya *us-east-1* dengan Wilayah yang ingin Anda daftarkan ID paket Perlindungan Malware.

```
aws guardduty list-malware-protection-plans --region us-east-1
```

Dukungan fitur Amazon S3

Tabel berikut menentukan apakah Perlindungan Malware untuk S3 mendukung fitur Amazon S3 yang terdaftar atau tidak.

Apakah dukungan tersedia?	Deskripsi
Ya	Objek S3 dapat diambil tanpa memulihkan secara asinkron.

Apakah dukungan tersedia?	Deskripsi
Bersyarat	• Dukungan Intelligent Tiering tersedia untuk objek S3 di tingkatan Akses Instans Sering, Jarang, dan Arsip. • Tingkat opt-in Archive dan Deep Archive tidak didukung. • Intelligent Tiering selalu membuat objek baru di tingkat Frequent Access. Oleh karena itu, pemindaian objek saat membuat didukung. • Fitur tiering Cerdas Masa Depan mungkin memulai objek di Arsip. Karena itu, ini tidak didukung.
Tidak	GuardDuty hanya mendukung bucket tujuan umum untuk Perlindungan Malware untuk S3.

Apakah dukungan tersedia?	Deskripsi
Tidak	Objek S3 harus dipulihkan sebelum dapat diakses.
Tidak	Perlindungan Malware untuk S3 tidak didukung di Outposts.
Ya	Semua objek S3 yang diunggah dipindai untuk malware. Jika Anda mengunggah objek dengan file versi v1 dan segera mengunggah versi lain yang diganti dengan v2, maka GuardDuty akan memindai file objek versi v1 dan v2. Namun, waktu mulai pemindaian mungkin tidak dalam urutan yang sama.

Apakah dukungan tersedia?	Deskripsi
Ya	Jika bucket tujuan adalah sumber daya yang dilindungi, maka GuardDuty akan memindai semua objek S3 yang direplikasi ke awalan yang dilindungi dan dipantau.
Tidak	Anda tidak dapat menentukan aturan replikasi berdasarkan tag hasil pemindaian. Amazon S3 tidak mendukung replikasi untuk tag, kecuali saat membuat.

Apakah dukungan tersedia?	Deskripsi
Ya	GuardDuty mendukung pemindaian malware untuk objek S3 yang dienkripsi dengan kunci yang dikelola dan dikelola pelanggan. Pastikan bahwa peran IAM mencakup izin untuk menggunakan kunci. Untuk informasi selengkapnya, lihat Menambahkan izin kebijakan IAM.
Tidak	Perlindungan Malware untuk S3 tidak mendukung pemindaian objek S3 yang dienkripsi dengan kunci yang tidak dapat diakses.

Apakah dukungan tersedia?	Deskripsi
Tidak	Saat objek Amazon S3 Anda dienkripsi dengan menggunakan Klien Enkripsi Amazon S3, objek Anda tidak akan terpapar ke pihak ketiga mana pun, termasuk. AWS Untuk informasi tentang alasan ini tidak didukung, lihat Melindungi data dengan menggunakan enkripsi sisi klien. **Note** CSE-KMS objek terenkripsi diterima sebagai gumpalan terenkripsi di mana enkripsi tidak dapat ditentukan. Oleh karena itu, GuardDuty memprosesnya saat diterima, dan memindai gumpalan terenkripsi sebagai file biasa. GuardDuty tidak mengembalikan status `UNSUPPORTED` pemindaian untuk objek tersebut, kecuali salah satu yang Kuota dalam Perlindungan Malware untuk S3 melebihi.
Ya	Objek S3 yang terkunci dikunci berdasarkan WORM - Tulis Setelah Membaca Banyak. Perlindungan Malware untuk S3 dapat mengakses dan memindai objek.
Ya	Perlindungan Malware untuk S3 dapat memindai bucket yang diatur dengan Requester Pays. Pemohon akan membayar untuk panggilan S3. Untuk informasi selengkapnya, lihat Menggunakan bucket Requester Pays untuk transfer penyimpanan dan penggunaan di Panduan Pengguna Amazon S3.

Apakah dukungan tersedia?	Deskripsi
Ya	Anda dapat menentukan kebijakan siklus hidup berdasarkan tag hasil pemindaian. Misalnya, hapus objek berbahaya secara otomatis. Untuk informasi selengkapnya tentang konfigurasi lifcycle, lihat Mengelola siklus hidup penyimpanan Anda di Panduan Pengguna Amazon S3.
Ya	Anda dapat menentukan kebijakan sumber daya bucket berdasarkan tag hasil pemindaian objek S3. Misalnya, mencegah akses ke objek S3 yang belum dipindai, atau ancaman yang GuardDuty terdeteksi. Untuk informasi selengkapnya, lihat Menggunakan kontrol akses berbasis tag (TBAC) dengan Perlindungan Malware untuk S3.
Tidak	Perlindungan Malware untuk S3 hanya memindai konten objek S3.

Kuota dalam Perlindungan Malware untuk S3

Bagian ini menyediakan kuota default, sering disebut sebagai batas. Kecuali ditentukan, setiap kuota adalah Region-specific. Untuk melihat kuota default khusus untuk menggunakan GuardDuty layanan dasar, lihatGuardDuty Kuota Amazon.

Tabel berikut menjelaskan beberapa kuota yang akan berlaku untuk Anda Akun AWS.

AWS nilai kuota default	Apakah itu dapat disesuaikan?	Deskripsi
100GB	Tidak	Ukuran objek S3 maksimum yang GuardDuty akan mencoba memindai malware.

AWS nilai kuota default	Apakah itu dapat disesuaikan?	Deskripsi
100,000	Tidak	Jumlah maksimum file yang GuardDuty dapat mengekstrak dan menganalisis dalam objek S3. **Note** Jenis file majemuk berpotensi tunduk pada batasan ini. Jenis file termasuk, tetapi tidak terbatas pada, pesan email yang dikodekan Multipurpose Internet Mail Extensions (MIME), file Compiled Python (PYC), file Compiled HTML Help (CHM), semua installer, dan dokumen OpenDocument Format (ODF). **Note** Objek S3 dengan rasio kompresi yang sangat tinggi antara ukuran objek S3 dan ukuran konten yang diekstraksi mungkin tunduk pada batasan bahkan jika file yang diekstraksi di bawah kuota ini.
100	Tidak	Tingkat maksimum bersarang yang GuardDuty dapat mengekstrak dalam objek S3.

AWS nilai kuota default	Apakah itu dapat disesuaikan?	Deskripsi
25	Tidak	Jumlah maksimum bucket S3 yang dapat Anda aktifkan Perlindungan Malware untuk S3. Batas kuota ini adalah per akun di setiap Wilayah.

GuardDuty Perlindungan Malware untuk AWS Pencadangan

Topik

- Gambaran umum
- Bagaimana cara kerja Perlindungan Malware untuk Backup?
- GuardDuty Perlindungan Malware untuk Cadangan: Izin Peran IAM
- (Opsional) Memulai Perlindungan Malware untuk Pencadangan Secara Independen (hanya konsol)
- Memulai On-Demand Scan untuk Perlindungan Malware untuk Backup
- Memantau status pemindaian dan hasil dalam Perlindungan Malware untuk Backup
- Kuota untuk Perlindungan Malware untuk Backup

Gambaran umum

Perlindungan Malware untuk Pencadangan membantu Anda mendeteksi potensi keberadaan malware dalam data cadangan dengan memindai sumber daya yang AWS dilindungi cadangan seperti snapshot Amazon EBS, AMI Amazon EC2, dan Poin Pemulihan Amazon S3. Saat AWS Backup membuat atau memperbarui sumber daya cadangan yang dilindungi, GuardDuty dapat melakukan pemindaian malware pada cadangan tersebut untuk membantu mengidentifikasi konten yang berpotensi berbahaya sebelum dikembalikan ke lingkungan Anda.

Bagaimana Anda dapat menggunakan Perlindungan Malware untuk Backup

Anda dapat menggunakan fitur ini dalam dua mode, tergantung pada apakah GuardDuty diaktifkan di akun Anda:

1. Menggunakan Perlindungan Malware untuk Backup dengan GuardDuty diaktifkan

   Bila GuardDuty diaktifkan di Wilayah, AWS Backup mengintegrasikan Perlindungan Malware dengan alur kerja GuardDuty temuan. Hasil pemindaian malware muncul dalam GuardDuty temuan selain Amazon EventBridge dan Amazon CloudWatch.
2. Menggunakan Perlindungan Malware untuk Backup tanpa mengaktifkan GuardDuty

   Anda dapat menggunakan Perlindungan Malware untuk Pencadangan secara mandiri, tanpa mengaktifkan GuardDuty layanan penuh. Dalam mode ini, hasil pemindaian tetap tersedia sepenuhnya melalui EventBridge dan CloudWatch.

Pertimbangan untuk menggunakan Perlindungan Malware untuk Backup secara independen

Saat menggunakan fitur tanpa mengaktifkan GuardDuty:

- Konfigurasi paket Backup dikelola sepenuhnya di AWS Backup.

GuardDuty tidak menyediakan kontrol untuk memilih paket cadangan, brankas, atau jenis sumber daya. Semua aktivasi, penjadwalan, dan konfigurasi kebijakan tetap ada di Backup AWS .

- GuardDuty Temuan tidak dihasilkan.

Temuan memerlukan ID detektor, yang dibuat hanya ketika GuardDuty diaktifkan. Saat menggunakan Perlindungan Malware secara independen, hasil pemindaian muncul secara eksklusif melalui EventBridge peristiwa dan CloudWatch metrik.

- Anda masih dapat memulai pemindaian sesuai permintaan dari konsol. GuardDuty

Bahkan ketika tidak GuardDuty diaktifkan, GuardDuty konsol menyediakan alur kerja untuk memulai pemindaian malware sesuai permintaan untuk jenis sumber daya cadangan yang didukung. Hal ini memungkinkan pelanggan untuk menggunakan GuardDuty antarmuka akrab tanpa memerlukan GuardDuty layanan penuh.

- Non-GuardDuty pelanggan dapat mengakses alur kerja inisiasi pemindaian.

Titik masuk pemindaian sesuai permintaan tersedia untuk semua pelanggan yang menggunakan Perlindungan Malware untuk Pencadangan, terlepas dari apakah ada GuardDuty detektor di akun.

- Perilaku dan cakupan pemindaian tetap identik.

Apakah GuardDuty diaktifkan atau tidak, fitur ini memindai jenis sumber daya AWS Backup yang sama dengan mesin deteksi malware yang sama. Satu-satunya perbedaan adalah di mana hasil dipublikasikan.

Model ini memungkinkan pelanggan untuk mengadopsi pemindaian malware untuk cadangan tanpa memerlukan GuardDuty fitur deteksi ancaman yang lebih luas, sambil tetap menyediakan GuardDuty-based alur kerja opsional untuk memulai dan melihat operasi pemindaian.

Cara Kerja Perlindungan Malware untuk Backup

Perlindungan Malware untuk Cadangan dapat memindai sumber daya yang dilindungi AWS Cadangan berikut:

- Snapshot Amazon EBS
- AMI Amazon EC2
- Poin Pemulihan Amazon S3 dan pencadangan berkelanjutan S3 atau pemulihan point-in-time- (PITR)
- Brankas terkunci (tidak dapat diubah) (EBS/EC2 Recovery Points) menggunakan AWS Backup Vault Lock di wilayah yang didukung

Pemindaian Inkremental

AWS Backup menangkap perubahan inkremental untuk banyak jenis sumber daya. GuardDuty memiliki kemampuan untuk memindai hanya blok atau objek baru atau yang diubah ketika cadangan dibuat atau diperbarui, meningkatkan kinerja dan mengurangi overhead pemindaian sambil mencapai cakupan penuh dari waktu ke waktu.

On-demand pemindaian

Anda dapat memulai pemindaian pada sumber cadangan yang didukung kapan saja—langsung dari AWS Backup atau konsol. GuardDuty Kasus penggunaan umum termasuk memverifikasi cadangan sebelum memulihkan, memeriksa ulang data lama setelah tanda tangan ancaman baru diterbitkan, atau melakukan pemindaian kepatuhan berkala.

> **Note**
>
> - Perlindungan Malware untuk Cadangan hanya dapat diaktifkan untuk sumber daya cadangan di Wilayah yang sama.
> - GuardDuty memindai salinan cadangan hanya-baca; itu tidak mengubah konten cadangan.
> - Pemindaian berfungsi untuk brankas standar dan brankas yang terkunci (tidak dapat diubah).

Bagaimana cara kerja Perlindungan Malware untuk Backup?

Bagian ini menjelaskan komponen Perlindungan Malware untuk Pencadangan, cara kerjanya, dan bagaimana Anda dapat meninjau status dan hasil pemindaian malware.

Gambaran umum

Perlindungan Malware untuk Cadangan adalah fitur yang membantu Anda mendeteksi keberadaan malware pada snapshot EBS, gambar EC2 (AMI), dan Poin Pemulihan milik jenis sumber daya EBS, EC2, dan S3. Anda dapat memulai pemindaian malware sesuai permintaan baik melalui GuardDuty konsol atau API dengan meneruskan peran IAM yang menyediakan izin yang diperlukan untuk pemindaian, bersama dengan satu atau dua ARN sumber daya tergantung pada kategori pemindaian. Ada dua kategori pemindaian yang mungkin - pemindaian penuh dan pemindaian tambahan.

Pemindaian penuh dan pemindaian Incremental

Pemindaian penuh adalah tempat API akan menerima ARN sumber daya dan memindai semua file dalam sumber daya itu. Pemindaian tambahan di sisi lain membutuhkan dua ARN sumber daya, keduanya milik sumber daya yang sama, dan memindai file yang diubah di antara mereka. Sebagai contoh, mari kita asumsikan kita mengambil snapshot dari volume EBS. Sebut saja snapshot-1. Jika pemindaian penuh dilakukan pada snapshot ini, GuardDuty memindai semua file yang terkandung dengan snapshot ini. Sekarang mari kita asumsikan bahwa beberapa file ditambahkan ke volume yang sama, dan snapshot baru diambil. Sebut saja snapshot-2. Karena hanya beberapa file yang berubah antara snapshot-1 dan snapshot-2, seseorang dapat memicu pemindaian tambahan dengan ARN sumber daya kedua snapshot ini. Dalam hal ini snapshot-2 disebut sebagai `target` sumber daya, dan snapshot-1 disebut sebagai sumber daya. `base` Anda akan melihat terminologi ini digunakan di sisa dokumen. Pemindaian inkremental ini akan memindai file yang diubah antara snapshot-1 dan snapshot-2.

Pemindaian Malware untuk Point-in-Time-Recovery (PITR)

Saat diaktifkan dari AWS Backup, pemindaian malware untuk pencadangan berkelanjutan atau PITR terjadi sesuai dengan frekuensi yang dikonfigurasi pada paket Backup. Ini diatur oleh layanan Backup AWS . Misalnya, GuardDuty akan menjalankan pemindaian pertama dari t0 ke t2, pemindaian berikutnya dari t2 ke t4, pemindaian berikutnya dari t4 ke t6 dan seterusnya. Masing-masing pemindaian ini menghasilkan ID pemindaian yang dapat ditanyakan menggunakan `GetMalwareScan` API untuk mendapatkan status dan hasil pemindaian untuk periode waktu tersebut.

Atau, Anda juga dapat memindai sumber daya PITR lengkap dari GuardDuty konsol atau dengan menggunakan GuardDuty `StartMalwareScan` API sesuai permintaan dengan meneruskan stempel waktu akhir. Ini akan memastikan bahwa GuardDuty memindai seluruh sumber daya dari awal, hingga stempel waktu akhir.

> **Note**
>
> - Anda tidak dapat memicu pemindaian sebagian atau inkremental pada PITR dari. GuardDuty
> - Stempel waktu akhir yang diteruskan untuk pemindaian sesuai permintaan tidak boleh lebih tua dari (waktu saat ini - 15 menit).

Memindai Ulang File yang Terinfeksi Sebelumnya dalam Pemindaian Inkremental

Sebagai bagian dari pemindaian tambahan, juga GuardDuty akan memindai ulang file yang sebelumnya terinfeksi dari pemindaian dasar hingga 365 hari.

Persyaratan untuk Pemindaian Inkremental

Persyaratan berikut harus dipenuhi GuardDuty untuk melakukan pemindaian tambahan. Jika salah satu persyaratan ini tidak terpenuhi, GuardDuty akan melewatkan pemindaian.

- Sumber daya dasar harus dipindai dalam 365 hari terakhir dan hasil pemindaian harus dalam `COMPLETED` atau`COMPLETED_WITH_ISSUES`.
- Sumber daya dasar harus memiliki tanggal pembuatan yang lebih awal dari sumber daya target.
- Sumber daya dasar dan target harus memiliki jenis enkripsi yang sama jika terjadi snapshot.
- Sumber daya dasar dan target harus dari garis keturunan yang sama.
  - Untuk snapshot EBS dan titik pemulihan EBS, ini berarti bahwa mereka berasal dari volume yang sama, atau salinan dari volume yang sama, tanpa perubahan dalam jenis enkripsi.
  - Untuk S3 Recovery Point, ARN sumber daya dasar dan target harus dibuat dari bucket S3 dasar yang sama.
  - Dalam kasus AMI, pasangan snapshot dibandingkan antara AMI dasar dan target untuk mengidentifikasi snapshot untuk pemindaian tambahan. Setiap pasang snapshot harus memenuhi kondisi yang disebutkan di atas. Setiap snapshot dalam AMI target yang tidak memiliki snapshot pencocokan yang sesuai di AMI dasar akan dilewati.

Re-scanning Sumber daya cadangan yang dipindai sebelumnya

Anda dapat memulai pemindaian malware sesuai permintaan baru pada sumber daya yang sama setelah 10 menit dari waktu mulai pemindaian malware sebelumnya. Jika pemindaian malware

baru dimulai dalam waktu 10 menit setelah inisiasi pemindaian malware sebelumnya, permintaan Anda akan menghasilkan kesalahan berikut, dan tidak ada ID pemindaian yang akan dihasilkan untuk permintaan ini. Langkah-langkah untuk memindai ulang instance tetap sama dengan memulai pemindaian malware sesuai permintaan untuk pertama kalinya.

Peran IAM Diperlukan untuk Pemindaian

Anda harus meneruskan peran IAM untuk memulai pemindaian penuh atau tambahan. Peran ini memberikan izin yang diperlukan untuk melakukan operasi pemindaian. GuardDuty Perlindungan Malware untuk Cadangan: Izin Peran IAMmenyediakan daftar persis izin yang diperlukan, bersama dengan kebijakan kepercayaan yang relevan yang diperlukan untuk melakukan pemindaian.

Meninjau status dan hasil pemindaian Sumber Daya

GuardDuty menerbitkan peristiwa hasil pemindaian ke bus acara EventBridge default Amazon. GuardDuty menggunakan pengiriman setidaknya sekali, yang berarti Anda mungkin menerima beberapa hasil pemindaian untuk objek yang sama. Kami merekomendasikan merancang aplikasi Anda untuk menangani hasil duplikat. Anda hanya ditagih sekali untuk setiap objek yang dipindai.

Untuk informasi selengkapnya, lihat Memantau status pemindaian dan hasil dalam Perlindungan Malware untuk Backup.

Meninjau temuan yang dihasilkan

Meninjau temuan tergantung pada apakah Anda menggunakan Perlindungan Malware untuk Pencadangan dengan GuardDuty atau tidak. Pertimbangkan skenario berikut:

Menggunakan Perlindungan Malware untuk Pencadangan saat Anda mengaktifkan GuardDuty layanan (ID detektor)

Jika pemindaian malware mendeteksi file yang berpotensi berbahaya dalam sumber Backup yang dipindai, GuardDuty akan menghasilkan temuan terkait. Anda dapat melihat detail temuan dan menggunakan langkah-langkah yang disarankan untuk berpotensi memulihkan temuan tersebut. Berdasarkan frekuensi temuan Ekspor Anda, temuan yang dihasilkan akan diekspor ke bucket S3 dan bus EventBridge acara Amazon.

Untuk informasi tentang jenis temuan yang akan dihasilkan, lihat Perlindungan Malware untuk jenis pencarian Backup menemukan jenis untuk Perlindungan Malware untuk Cadangan.

Menggunakan Perlindungan Malware untuk Backup sebagai fitur independen (tidak ada ID detektor)

GuardDuty tidak akan dapat menghasilkan temuan karena tidak ada ID detektor terkait. Untuk mengetahui status pemindaian sumber daya cadangan, Anda dapat melihat hasil pemindaian yang GuardDuty secara otomatis dipublikasikan ke bus acara default Anda.

Untuk informasi tentang status dan hasil pemindaian, lihatMemantau status pemindaian dan hasil dalam Perlindungan Malware untuk Backup.

> **Note**
>
> Jika Anda juga menggunakan Perlindungan Malware untuk S3, ada kemungkinan bahwa file S3 Anda sebelumnya ditandai sebagai NO_THREATS_FOUND namun file yang sama dapat muncul dalam daftar ancaman untuk Titik Pemulihan Cadangan yang dimiliki objek tersebut. Ini terjadi karena layanan sering memperbarui tanda tangan malware, yang mungkin telah mengubah status file. Harap dicatat bahwa dalam kasus seperti itu GuardDuty tidak kembali dan memperbarui tag pada file di ember S3 asli. Satu-satunya cara untuk mendapatkan tag yang diperbarui diterapkan pada file adalah dengan mengunggah ulang objek ke bucket atau menggunakan fitur pemindaian sesuai permintaan untuk S3.

GuardDuty Perlindungan Malware untuk Cadangan: Izin Peran IAM

Peran pelanggan disediakan untuk pemindaian malware

GuardDuty Perlindungan Malware mengharapkan peran pelanggan (peran pemindai) diberikan saat pemindaian dimulai pada sumber daya Backup, yaitu snapshot, AMI, dan Recovery Points. EBS/EC2/S3 Peran ini memberikan izin yang diperlukan GuardDuty untuk melakukan pemindaian pada sumber daya tertentu tersebut. Kebijakan izin dan kebijakan kepercayaan untuk peran ini dapat ditemukan dilzin dan kebijakan kepercayaan untuk peran. Bagian di bawah ini menjelaskan mengapa masing-masing izin ini diperlukan.

Detail tentang izin

- `ModifySnapshotAttribute`- Memungkinkan snapshot terenkripsi kunci terenkripsi yang tidak terenkripsi dan dikelola pelanggan untuk diakses oleh akun layanan Perlindungan Malware. GuardDuty
- `CreateGrant`- Memungkinkan Perlindungan GuardDuty Malware untuk membuat dan mengakses volume EBS terenkripsi Kunci Terkelola Pelanggan dari snapshot terenkripsi kunci yang dikelola pelanggan yang disediakan akses ke akun GuardDuty layanan.

- `RetireGrant`- Memungkinkan Perlindungan GuardDuty Malware untuk menghentikan hibah yang dibuat pada Kunci Dikelola Pelanggan untuk membaca snapshot terenkripsi
- `ReEncryptTo`dan `ReEncryptFrom` - Diperlukan oleh EBS untuk memberikan GuardDuty akses ke snapshot yang dienkripsi dengan kunci yang dikelola pelanggan dan membuat volume terenkripsi dari mereka. Meskipun pelanggan mungkin menganggap ReEncryption snapshot selama berbagi sebagai transisi utama, snapshot tetap tidak berubah dari perspektif pelanggan setelah dibuat.
- `ListSnapshotBlocks`dan `GetSnapshotBlock` - EBS Direct API digunakan untuk mengakses blok snapshot untuk snapshot terenkripsi Kunci AWS Terkelola. Ini dilakukan karena snapshot terenkripsi Kunci AWS Terkelola tidak dapat diakses lintas akun.
- `Decrypt`- Memungkinkan mendekripsi snapshot dasar yang merupakan kunci yang dikelola pelanggan yang dienkripsi saat diunduh ke memori menggunakan EBS Direct API sebagai bagian dari pemindaian tambahan.
- `ListChangedBlocks`- EBS Direct API digunakan dalam pemindaian snapshot tambahan untuk mendapatkan daftar blok yang diubah antara dua snapshot.
- `DescribeKey`- Memungkinkan Perlindungan GuardDuty Malware untuk menentukan KeyID dari kunci yang AWS dikelola di akun pelanggan.
- `DescribeImages`- Memungkinkan AMI dijelaskan untuk mendapatkan daftar snapshot milik AMI.
- `DescribeRecoveryPoint`- Memungkinkan layanan untuk mengambil rincian Recovery Point dan memverifikasi jenis sumber daya untuk Recovery Point.
- `CreateBackupAccessPoint`,`DescribeBackupAccessPoint`, `DeleteBackupAccessPoint` - Memungkinkan layanan untuk membuat, mendeskripsikan, dan menghapus Access Point yang diperlukan untuk mengakses Recovery Points.
- `kms:Decrypt`- Memungkinkan layanan untuk mengakses objek di S3 Recovery Point selama S3 Recovery Point scan.

Mengamankan Peran

Peran tersebut harus dikonfigurasi dengan kebijakan kepercayaan yang mempercayai prinsip layanan Perlindungan GuardDuty Malware. Ini memastikan bahwa tidak ada prinsipal selain GuardDuty layanan yang dapat mengambil peran ini. Selanjutnya, Anda didorong untuk meringkas kebijakan ke sumber daya tertentu alih-alih*. Ini termasuk id snapshot dan id kunci. Melakukan hal ini akan memastikan bahwa peran tersebut hanya menyediakan akses ke sumber daya tertentu tersebut.

> **Important**
>
> Konfigurasi yang salah dapat mengakibatkan kegagalan pemindaian karena izin yang tidak mencukupi.

Bagaimana Perlindungan GuardDuty Malware menggunakan hibah di AWS KM

GuardDuty Perlindungan Malware membutuhkan hibah untuk menggunakan kunci KMS Anda.

Saat Anda memulai pemindaian pada snapshot terenkripsi atau AMI EC2 yang terdiri dari snapshot terenkripsi, Perlindungan GuardDuty Malware membuat hibah atas nama Anda dengan mengirimkan permintaan ke KMS. CreateGrant AWS Hibah ini memberikan GuardDuty akses ke kunci tertentu di akun Anda.

GuardDuty Perlindungan Malware memerlukan hibah untuk menggunakan kunci yang dikelola pelanggan Anda untuk operasi internal berikut:

- Kirim DescribeKeypermintaan AWS untuk mengambil detail tentang kunci terkelola pelanggan simetris yang dienkripsi oleh sumber daya yang dikirimkan untuk pemindaian malware.
- Buat volume EBS dari snapshot terenkripsi menggunakan CreateVolumeAPI dan enkripsi volume dengan kunci yang sama.
- Akses blok snapshot pada snapshot melalui GetSnapshotBlockAPI selama pemindaian tambahan.
- Kirim permintaan Dekripsi ke AWS KMS untuk mendekripsi kunci data terenkripsi sehingga mereka dapat digunakan untuk membaca data pada snapshot selama pemindaian.

Anda dapat mencabut hibah yang dibuat, atau menghapus akses layanan ke kunci yang dikelola pelanggan kapan saja. Jika Anda melakukannya, GuardDuty tidak akan dapat mengakses data apa pun yang dienkripsi oleh kunci yang dikelola pelanggan, yang memengaruhi operasi yang bergantung pada data tersebut.

GuardDuty Konteks Enkripsi Perlindungan Malware

Konteks enkripsi adalah kumpulan opsional pasangan kunci-nilai yang berisi informasi kontekstual tambahan tentang data.

Saat Anda menyertakan konteks enkripsi dalam permintaan untuk mengenkripsi data, AWS KMS; mengikat konteks enkripsi ke data terenkripsi. Untuk mendekripsi data, Anda menyertakan konteks enkripsi yang sama dalam permintaan.

GuardDuty Perlindungan Malware menggunakan salah satu dari dua konteks enkripsi.

Konteks Enkripsi 1: Kuncinya adalah`aws:guardduty:id`.

```
"encryptionContext": {
    "aws:guardduty:id": "snap-11112222333344"
}
```

Konteks enkripsi ini digunakan dengan operasi hibah: CreateGrant, Dekripsi,,, GenerateDataKeyWithoutPlaintext ReEncryptTo, RetireGrant. DescribeKey

Satu hibah dibuat pada sumber daya saat ini dengan konteks enkripsi ini dan operasi hibah.

Konteks Enkripsi 2: Kuncinya adalah `aws:ebs:id`

```
"encryptionContext": {
    "aws:ebs:id": "snap-11112222333344"
}
```

Konteks enkripsi ini digunakan dengan operasi hibah: ReEncryptFrom, Dekripsi,, RetireGrant. DescribeKey

Tiga hibah dibuat dengan konteks enkripsi dan operasi hibah ini. Satu di snapshot target dengan operasi `ReEncryptFrom` hibah. Yang kedua pada snapshot target dengan `Decrypt, RetireGrant, DescribeKey` operasi. Dan yang ketiga pada snapshot dasar dengan operasi hibah yang sama dengan hibah kedua.

Izin dan kebijakan kepercayaan untuk peran

Kebijakan Izin

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
```

```
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Sid": "CreateGrantPermissions",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "kms:EncryptionContext:aws:guardduty:id": "snap-*",
                    "kms:ViaService": [
                        "guardduty.*.amazonaws.com",
                        "backup.*.amazonaws.com"
                    ]
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "CreateGrant",
                        "GenerateDataKeyWithoutPlaintext",
                        "ReEncryptFrom",
                        "ReEncryptTo",
                        "RetireGrant",
                        "DescribeKey"
                    ]
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Sid": "CreateGrantPermissionsForReEncryptAndDirectAPIs",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "kms:EncryptionContext:aws:ebs:id": "snap-*",
                    "kms:ViaService": [
                        "guardduty.*.amazonaws.com",
                        "backup.*.amazonaws.com"
```

```
                ]
            },
            "ForAllValues:StringEquals": {
                "kms:GrantOperations": [
                    "Decrypt",
                    "ReEncryptTo",
                    "ReEncryptFrom",
                    "RetireGrant",
                    "DescribeKey"
                ]
            },
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeImages",
            "ec2:DescribeSnapshots"
        ],
        "Resource": "*"
    },
    {
        "Sid": "ShareSnapshotPermission",
        "Effect": "Allow",
        "Action": [
            "ec2:ModifySnapshotAttribute"
        ],
        "Resource": "arn:aws:ec2:*:*:snapshot/*"
    },
    {
        "Sid": "ShareSnapshotKMSPermission",
        "Effect": "Allow",
        "Action": [
            "kms:ReEncryptTo",
            "kms:ReEncryptFrom"
        ],
        "Resource": "arn:aws:kms:*:*:key/*",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "ec2.*.amazonaws.com"
            }
```

```
            }
        },
        {
            "Sid": "DescribeKeyPermission",
            "Effect": "Allow",
            "Action": "kms:DescribeKey",
            "Resource": "arn:aws:kms:*:*:key/*"
        },
        {
            "Sid": "DescribeRecoveryPointPermission",
            "Effect": "Allow",
            "Action": [
                "backup:DescribeRecoveryPoint"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateBackupAccessPointPermissions",
            "Effect" : "Allow",
            "Action" : [
                "backup:CreateBackupAccessPoint"
            ],
            "Resource": "arn:aws:backup:*:*:recovery-point:*"
        },
        {
            "Sid": "ReadAndDeleteBackupAccessPointPermissions",
            "Effect" : "Allow",
            "Action" : [
                "backup:DescribeBackupAccessPoint",
                "backup:DeleteBackupAccessPoint"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSKeyPermissionsForInstantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "backup.*.amazonaws.com"
                }
```

```
            }
        }
    ]
}
```

Kebijakan Kepercayaan

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

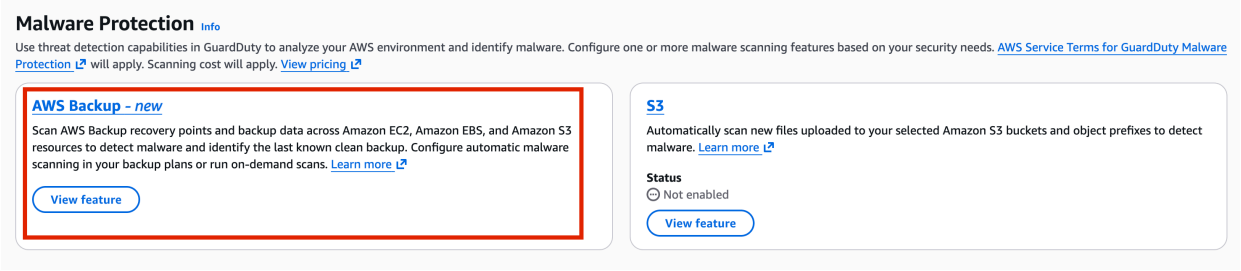
(Opsional) Memulai Perlindungan Malware untuk Pencadangan Secara Independen (hanya konsol)

Gunakan langkah opsional ini saat Anda ingin memulai opsi deteksi ancaman Perlindungan Malware untuk Cadangan terlepas dari GuardDuty status di AWS akun Anda.

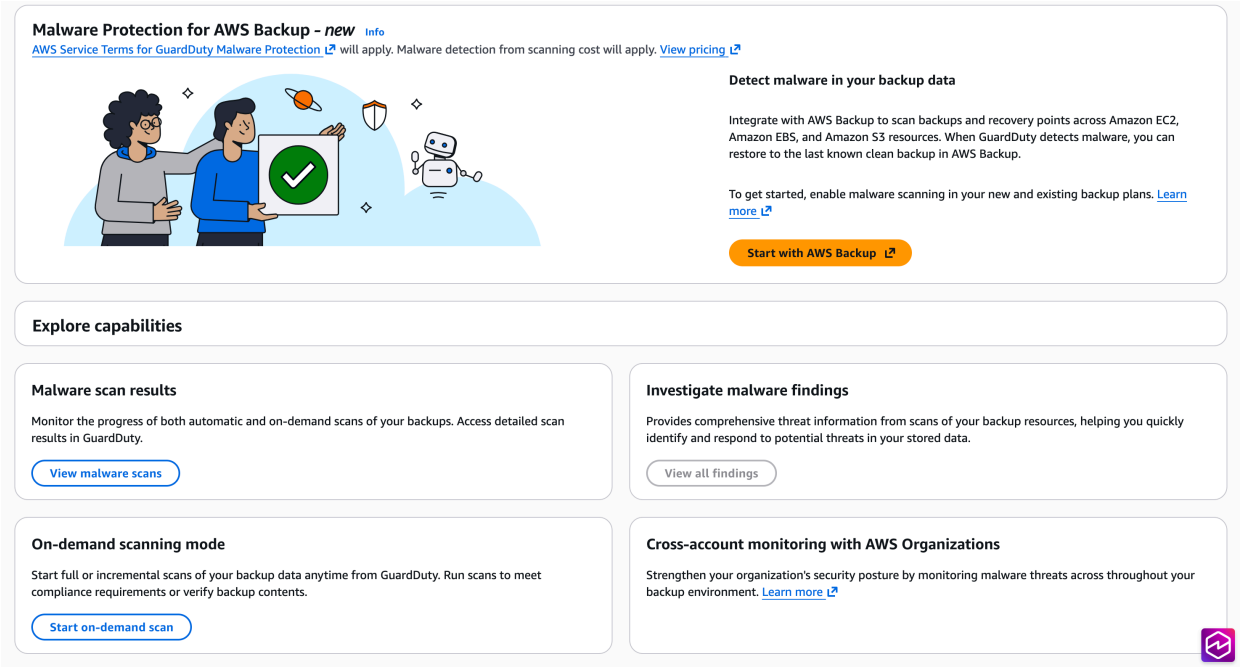
Jika Anda juga ingin menggunakan paket perlindungan khusus lainnya di GuardDuty, Anda harus memulai dengan GuardDuty layanan Amazon. Untuk informasi tentang rencana GuardDuty perlindungan, lihat Fitur dari GuardDuty.

Langkah-langkah untuk memulai dengan Perlindungan Malware untuk Backup

1. Masuk ke Konsol AWS Manajemen dan buka https://console.aws.amazon.com/guardduty/konsol di https://console.aws.amazon.com/guardduty/
2. Pilih Temukan Fitur Perlindungan Malware dan klik Memulai.
3. Saat mengklik Mulai, Anda dapat memilih di antara opsi termasuk fitur AWS Backup dan S3 Malware Protection.



4. Anda akan dibawa ke halaman Perlindungan Malware untuk Cadangan, di mana Anda dapat memilih untuk Memulai pemindaian sesuai permintaan atau Melihat pemindaian malware.



Memulai On-Demand Scan untuk Perlindungan Malware untuk Backup

Konsol

1. Masuk ke Konsol AWS Manajemen dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Arahkan ke Perlindungan Malware untuk Pencadangan dan klik Mulai pemindaian sesuai permintaan.
3. Pilih antara Full Scan dan Incremental Scan.

1. Untuk memulai pemindaian penuh, masukkan ARN sumber daya dari sumber daya yang akan dipindai.
2. Untuk pemindaian tambahan, masukkan ARN Sumber Daya Target dan ARN Sumber Daya Dasar.
3. Jika sumber daya yang dipindai adalah Titik Pemulihan, Anda juga harus memasukkan nama Brankas AWS Cadangan miliknya.
4. Untuk sumber daya S3 PITR, berikan stempel waktu akhir. Stempel waktu akhir tidak boleh lebih tua dari (waktu saat ini - 15 menit).

4. Akses layanan - Anda harus memilih peran yang memiliki izin yang diperlukan untuk mengakses sumber daya dan melakukan pemindaian. Klik Lihat Kebijakan untuk melihat izin persis yang diperlukan untuk peran tersebut, bersama dengan kebijakan kepercayaan yang diperlukan.

Anda dapat membuat perubahan pada kebijakan berdasarkan persyaratan atau cakupan izin ke sumber daya yang tepat. Untuk detail selengkapnya tentang cara membuat atau memperbarui peran IAM, lihatGuardDuty Perlindungan Malware untuk Cadangan: Izin Peran IAM.

Untuk masalah dengan izin peran IAM, lihat Kesalahan pemecahan masalah izin peran IAM.

API/CLI

Invoke StartMalwareScanyang menerima sumber daya tempat Anda ingin memulai pemindaian malware sesuai permintaan. `resourceArn` Jika Anda ingin memulai pemindaian inkremental, teruskan masuk. `baselineResourceArn` `incrementalScanDetails` Sebagai bagian dari konfigurasi pemindaian, Anda juga perlu memberikan peran IAM yang memiliki semua izin yang diperlukan untuk memulai pemindaian. Jika sumber daya yang dipindai adalah sumber daya S3 PITR, Anda harus meneruskan stempel waktu akhir. Setelah Anda berhasil memulai pemindaian, `StartMalwareScan` mengembalikan file`scanId`. Panggil `GetMalwareScan` API untuk memantau kemajuan pemindaian yang dimulai dan untuk mendapatkan detail pemindaian setelah selesai.

Memantau status pemindaian dan hasil dalam Perlindungan Malware untuk Backup

Setelah pemindaian malware dimulai, GuardDuty berikan beberapa mekanisme di mana Anda dapat memantau status dan hasil pemindaian. Tabel berikut memberikan beberapa nilai yang terkait dengan pemindaian malware.

Nilai potensial
`RUNNING`, `COMPLETED` `COMPLETED_WITH_ISSUES` ,`FAILED`, atau `SKIPPED`
`FULL_SCAN` atau `INCREMENTAL_SCAN`
`GUARDDUTY_INITIATED` , `ON_DEMAND` atau `BACKUP_INITIATED`
`NO_THREATS_FOUND` atau `THREATS_FOUND`

*Perhatikan bahwa Status Hasil Pemindaian mungkin tidak ada jika pemindaian tidak selesai. Status Hasil Pemindaian THREATS_FOUND menunjukkan bahwa GuardDuty mendeteksi keberadaan malware.

Untuk Poin Pemulihan S3, COMPLETED_WITH_ISSUES menunjukkan bahwa beberapa file dilewati atau gagal. Untuk AMI, COMPLETED_WITH_ISSUES menunjukkan bahwa setidaknya 1 snapshot tidak dapat dipindai. Lihat di bawah untuk daftar alasan yang dilewati.

Pemindaian juga dapat dilewati karena berbagai alasan. Tabel di bawah ini menjelaskan alasan mengapa pemindaian dapat dilewati:

Alasan
Peran Pelanggan tidak memiliki izin yang diperlukan untuk layanan untuk melakukan pemindaian

Alasan
Sumber daya yang mencoba dipindai tidak ada di akun atau dihapus selama pemindaian
Ukuran snapshot lebih besar dari yang saat ini didukung oleh GuardDuty
Sumber daya yang ditentukan dalam permintaan pemindaian tambahan tidak memiliki perbedaan
Sumber daya tidak dalam keadaan yang diharapkan. Jika pemindaian bersifat inkremental, titik pemulihan dasar tidak dalam keadaan TERSEDIA atau SELESAI
Untuk pemindaian tambahan - basis dan sumber daya saat ini bukan dari garis keturunan yang sama
Untuk pemindaian tambahan - sumber daya dasar sebelumnya tidak dipindai atau tidak ada pemindaian lengkap yang ditemukan
Untuk pemindaian tambahan - tanggal pembuatan sumber daya dasar lebih besar dari tanggal pembuatan sumber daya saat ini
Jenis sumber daya yang diminta tidak mendukung pemindaian inkremental

Alasan
AMI publik, AMI dengan hanya penyimpanan sementara, dan AMI tidak dalam status tersedia tidak memenuhi syarat untuk pemindaian
Snapshot penyimpanan dingin tidak memenuhi syarat untuk pemindaian
Pemindaian tidak didukung untuk jenis sumber daya komposit
Sumber daya yang diminta berisi kode produk Amazon Marketplace yang tidak mendukung pemindaian
AMI tidak mendukung pemindaian lebih dari 40 snapshot
Tidak ada pemetaan perangkat blok Ebs yang ditemukan untuk sumber daya yang diminta
Untuk pemindaian tambahan - arn sumber daya dasar berbeda dari arn sumber daya yang diharapkan
Semua file dalam pemindaian dilewati atau gagal

Hasil pemindaian memiliki periode retensi 90 hari. Pilih metode akses pilihan Anda untuk melacak status pemindaian malware Anda.

Memantau Pemindaian Menggunakan Konsol

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Pemindaian malware.
3. Anda dapat memfilter pemindaian malware dengan Properti berikut yang tersedia di bilah pencarian filter.

   - Scan ID — Pengidentifikasi unik yang terkait dengan pemindaian malware.
   - ID Akun — Akun tempat pemindaian malware dimulai.
   - Sumber daya ARN - Nama Sumber Daya Amazon (ARN) yang terkait dengan sumber daya Amazon yang terkait dengan pemindaian.
   - Jenis Sumber Daya — Jenis sumber daya yang terkait dengan pemindaian, seperti Instans EC2, Snapshot EBS | EC2 AMI, EBS Recovery Point, EC2 Recovery Point, atau S3 Recovery Point.
   - Status — Status pemindaian pemindaian, seperti Berjalan, Dilewati, Selesai, Selesai dengan Masalah, atau Gagal.
   - Jenis Pemindaian — Menunjukkan apakah ini pemindaian On-demand GuardDuty-initiated,, atau Backup-Initiated malware.

Pemantauan Pemindaian menggunakan API/CLI

- Anda dapat meminta ListMalwareScans untuk memfilter pemindaian malware dengan`RESOURCE_ARN`,,`SCAN_ID`,`ACCOUNT_ID`,, `SCAN_TYPE GUARDDUTY_FINDING_ID` `SCAN_STATUS`RESOURCE_TYPE, dan. `SCAN_START_TIME` Anda juga dapat meminta GetMalwareScan untuk mengambil metadata yang lebih rinci dari pemindaian dengan memberikan scan-id sebagai input. Kriteria `GUARDDUTY_FINDING_ID` filter `SCAN_TYPE` tersedia saat GuardDuty dimulai.
- Anda dapat mengubah contoh *`filter-criteria`* dalam perintah di bawah ini, dan dapat memfilter berdasarkan satu `CriterionKey` per satu. Pilihan untuk `CriterionKey` adalah`Resource_ARN`,`SCAN_ID`,`ACCOUNT_ID`,`SCAN_TYPE`, `GUARDDUTY_FINDING_ID`SCAN_STATUS,`RESOURCE_TYPE`, dan`SCAN_START_TIME`. Anda dapat mengubah *`max-results`* (hingga 50) dan*`sort-criteria`*. `AttributeName`Bidang ini wajib untuk `sort-criteria` dan harus diatur ke`scanStartTime`. Dalam contoh berikut,

nilai-nilai di *red* adalah placeholder. Ganti dengan nilai yang sesuai untuk akun Anda. Jika Anda menggunakan yang sama `CriterionKey` seperti di bawah ini untuk ListMalwareScans, pastikan untuk mengganti contoh `EqualsValue` dengan yang ingin *resource-type* Anda filter.

```
aws guardduty list-malware-scans --max-results 25 --sort-criteria
 '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"RESOURCE_TYPE", "FilterCondition":
{"EqualsValue":"EBS_SNAPSHOT"}}] }'
```

```
aws guardduty get-malware-scan --scan-id abc123
```

- Respons untuk perintah di atas untuk ListMalwareScans akan mengembalikan hingga 25 pemindaian dengan beberapa detail tentang sumber daya yang terpengaruh. Respons untuk perintah di atas untuk GetMalwareScan akan mengembalikan pemindaian tunggal dengan metadata rinci tentang pemindaian.

Pemantauan Pemindaian menggunakan EventBridge

Amazon EventBridge adalah layanan bus acara tanpa server yang memudahkan untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. EventBridge mengirimkan aliran data real-time dari aplikasi Anda sendiri, aplikasi Software-as-a-Service (SaaS), dan layanan Amazon serta merutekan data tersebut ke target seperti Lambda. Hal ini memungkinkan Anda memantau kejadian yang terjadi dalam layanan, dan membangun arsitektur yang didorong kejadian. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

GuardDuty menerbitkan EventBridge pemberitahuan ke bus acara default setelah status pemindaian ditentukan. Anda dapat mengatur EventBridge aturan di akun Anda untuk mengirim acara ke layanan lain yang terintegrasi dengan Amazon EventBridge. EventBridge Harga standar akan berlaku. Untuk informasi selengkapnya, lihat EventBridge harga Amazon.

Banyak nilai yang ditunjukkan di bawah ini adalah placeholder untuk contoh dan akan bervariasi tergantung pada pemindaian.

Peristiwa Hasil Pemindaian Malware

Nilai tipe detail potensial untuk Backup:

- “Perlindungan GuardDuty Malware Hasil Pemindaian Snapshot EBS”
- “Hasil Pemindaian AMI EC2 Perlindungan GuardDuty Malware”

- “Hasil Pemindaian Titik Pemulihan S3 Perlindungan GuardDuty Malware”
- “Perlindungan GuardDuty Malware Hasil Pemindaian Titik Pemulihan EBS”
- “Hasil Pemindaian Titik Pemulihan EC2 Perlindungan GuardDuty Malware”

Contoh Pola Acara:

```
{
      "detail-type": ["GuardDuty Malware Protection EC2 AMI Scan Result"],
      "source": ["aws.guardduty"]
}
```

Contoh Skema Pemberitahuan untuk Pemindaian AMI EC2 tanpa Ancaman Ditemukan:

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
    "source": "aws.guardduty",
    "account": "1111222233334444",
    "time": "2025-11-01T00:00:00Z",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/
ami-1234567890abcdef0"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "EC2_AMI",
        "scanId": "d41d8cd98f00b204e9800998ecf8427e",
        "scanStatusReason": null,
        "scanType": "ON_DEMAND",
        "triggerType": "GUARDDUTY",
        "scanCategory": "FULL_SCAN",
        "scanStartTime": 1234567890123,
        "scanCompleteTime": 2345678901234,
        "scanResultDetails": {
            "scanResultStatus": "NO_THREATS_FOUND",
            "uniqueThreatCount": null
        }
    }
}
```

Contoh Skema Pemberitahuan untuk Pemindaian AMI EC2 dengan Ancaman Ditemukan:


```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
    "source": "aws.guardduty",
    "account": "1111222233334444",
    "time": "2025-11-01T00:00:00Z",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/
ami-1234567890abcdef0"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "EC2_AMI",
        "scanId": "d41d8cd98f00b204e9800998ecf8427e",
        "scanStatusReason": null,
        "scanType": "ON_DEMAND",
        "triggerType": "GUARDDUTY",
        "scanCategory": "FULL_SCAN",
        "scanStartTime": 1234567890123,
        "scanCompleteTime": 2345678901234,
        "scanResultDetails": {
            "scanResultStatus": "THREATS_FOUND",
            "uniqueThreatCount": 1,
            "threats": {
                "name": "EICAR-Test-File (not a virus)",
                "source": "AMAZON",
                "count": 2,
                "itemDetails": [{
                    "resourceArn": "arn:aws:ec2:us-east-1:1111222233334444:snapshot/
snap-abcdef01234567890",
                    "hash":
 "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
                    "itemPath": "/eicar.txt",
                    "additionalInfo": {
                        "versionId": null,
                        "deviceName": "/dev/sdf"
                    }
                }]
            }
        }
    }
```

```
}
```

Contoh Skema Pemberitahuan untuk Pemindaian AMI EC2 yang Dilewati:

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
    "source": "aws.guardduty",
    "account": "1111222233334444",
    "time": "2025-11-01T00:00:00Z",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/
ami-1234567890abcdef0"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "EC2_AMI",
        "scanId": "d41d8cd98f00b204e9800998ecf8427e",
        "scanStatusReason": "UNSUPPORTED_AMI",
        "scanType": "ON_DEMAND",
        "triggerType": "GUARDDUTY",
        "scanCategory": "FULL_SCAN",
        "scanStartTime": 1234567890123,
        "scanCompleteTime": 2345678901234,
       "scanResultDetails": {
            "uniqueThreatCount": null,
            "threats": null
        }
    }
}
```

Kuota untuk Perlindungan Malware untuk Backup

Perlindungan Malware untuk kuota Backup

Nama kuota	AWS nilai kuota default	Apakah itu dapat disesuaikan?	Deskripsi
StartMalwareScan Batas TPS untuk semua jenis sumber daya	10	Tidak	
Ukuran snapshot maks didukung	2 TiB	Tidak	Batas ini berlaku untuk ukuran snapshot penuh (`fullSnapshotSizeInBytes`), bukan ukuran snapshot tambahan. Untuk informasi selengkapnya, lihat Snapshot di Referensi API Amazon EC2. Untuk pemindaian tambahan, GuardDuty lewati pemindaian jika snapshot saat ini atau snapshot dasar melebihi batas ini.
Sistem file yang didukung untuk pemindaian snapshot dan AMI	• Sistem File Teknologi Baru (NTFS) • Sistem File X (XFS) • Sistem File kedua diperpanjang (ext2) • Sistem File diperpanj	Tidak	

Nama kuota	AWS nilai kuota default	Apakah itu dapat disesuaikan?	Deskripsi
	ang keempat (ext4) • Sistem File Tabel Alokasi File (FAT) • Sistem File Tabel Alokasi File Virtual (VFAT)		
Jumlah maksimal snapshot dalam AMI yang didukung untuk pemindaian malware	40 untuk pemindaian penuh. Jika ada lebih dari 40, hanya GuardDuty akan memindai 40 di antara semua snapshot. Untuk pemindaian tambahan, pemindaian dilewati.	Tidak	
Ukuran maksimal objek dalam S3 Recovery Point	100 GB	Tidak	Ukuran objek S3 maksimum yang GuardDuty akan mencoba memindai malware.

Nama kuota	AWS nilai kuota default	Apakah itu dapat disesuaikan?	Deskripsi
Byte arsip yang diekstraksi	100 GB	Tidak	Jumlah maksimum data yang GuardDuty dapat mengekstrak dan menganalisis dari file arsip. GuardDuty akan melewati file arsip yang mengekstrak hingga lebih dari 100 GB.
File arsip yang diekstrak	10.000	Tidak	Jumlah maksimum file yang GuardDuty dapat mengekstrak dan menganalisis dalam file arsip. Jika arsip berisi lebih dari 10.000 file, maka GuardDuty harus melewati file yang diarsipkan. **Note** Jenis file majemuk berpotensi tunduk pada batasan ini. Jenis file termasuk, tetapi tidak terbatas pada, pesan email yang disandikan Multipurpose Internet Mail Extensions (MIME), file Compilated Python (PYC), file Compilated HTML Help (CHM), semua installer , dan dokumen Format (ODF). OpenDocument

Nama kuota	AWS nilai kuota default	Apakah itu dapat disesuaikan?	Deskripsi
Tingkat kedalaman arsip maksimum	5	Tidak	Tingkat maksimum arsip bersarang yang GuardDuty dapat mengekstrak. Jika arsip menyertakan file yang bersarang di luar nilai ini, maka GuardDuty akan melewati file bersarang tersebut.

GuardDuty Perlindungan RDS

> **Note**
>
> Anda dapat mengonfigurasi Perlindungan RDS bersama dengan semua paket perlindungan lainnya dari satu halaman di GuardDuty konsol. Untuk informasi selengkapnya, lihat Mengkonfigurasi rencana perlindungan.

Perlindungan RDS di Amazon GuardDuty menganalisis dan memprofilkan login RDS dan aktivitas data untuk potensi ancaman terhadap Amazon Aurora dan RDS Anda untuk database PostgreSQL.

Perlindungan RDS untuk aktivitas login menganalisis peristiwa login untuk potensi ancaman akses ke Amazon Aurora (Amazon Aurora MySQL-Compatible Edition dan Aurora Edition), RDS untuk PostgreSQL, Amazon RDS for MySQL, dan Amazon RDS for MariaDB database. PostgreSQL-Compatible Ini membantu Anda mengidentifikasi perilaku login yang berpotensi mencurigakan pada database yang didukung ini. GuardDutyterus memantau dan profil Aktivitas login RDS untuk aktivitas anomali. Misalnya, aktor eksternal yang sebelumnya tidak terlihat memiliki akses tidak sah ke database Anda, atau musuh mencoba akses brute-force dengan menebak kata sandi database.

Perlindungan RDS untuk aktivitas data menganalisis pola kueri database di Amazon Aurora untuk PostgreSQL dan RDS untuk database PostgreSQL untuk mendeteksi potensi akses data dan ancaman manipulasi. GuardDuty terus memantau dan membuat profil Aktivitas data RDS untuk perilaku anomali. Misalnya, seorang aktor membaca baris secara signifikan lebih banyak dari biasanya untuk database atau pengguna tersebut, menghapus atau menjatuhkan data, atau mengakses database Anda dari alamat IP berbahaya atau Tor yang diketahui.

Untuk akun yang belum mengaktifkan Perlindungan RDS, Anda dapat mempelajari lebih lanjut tentang 30-day free trial dan memilih untuk mengaktifkan fitur ini. Untuk mengaktifkan fitur ini, lihat Mengaktifkan Perlindungan RDS di lingkungan multi-akun atauMengaktifkan Perlindungan RDS untuk akun mandiri.

> **Catatan**
>
> RDS untuk instance replika baca PostgreSQL memerlukan instance database utama berada pada versi database yang didukung, dan berhasil direplikasi dari database utama. Untuk

informasi tentang replika baca, lihat Bekerja dengan replika baca instans DB di Panduan Pengguna Amazon RDS.

Perlindungan RDS tidak memerlukan infrastruktur tambahan dan dirancang agar tidak memengaruhi kinerja instans basis data Anda. Ketika RDS Protection mendeteksi upaya login, eksfiltrasi, atau aktivitas destruktif data yang berpotensi mencurigakan atau anomali, GuardDuty menghasilkan satu atau lebih dengan detail tentang database yang berpotensi dikompromikan. Jenis temuan Perlindungan RDS

Uji coba gratis 30 hari

- Saat Anda mengaktifkan GuardDuty di Wilayah baru untuk pertama kalinya, Anda menerima uji coba gratis 30 hari. Akun AWS Dalam hal ini, GuardDuty juga memungkinkan Perlindungan RDS, yang termasuk dalam uji coba gratis. Pemantauan aktivitas login Perlindungan RDS dan pemantauan aktivitas data Perlindungan RDS akan mulai memantau aktivitas database Anda.
- Ketika Anda sudah menggunakan GuardDuty dan memutuskan untuk mengaktifkan Perlindungan RDS di Wilayah baru untuk pertama kalinya, akun Anda di Wilayah ini akan mendapatkan uji coba gratis 30 hari untuk Perlindungan RDS.
- Ketika Anda sudah menggunakan Perlindungan RDS untuk aktivitas login Akun AWS dan memutuskan untuk mengaktifkan Perlindungan RDS untuk aktivitas data untuk pertama kalinya, akun Anda akan mendapatkan uji coba gratis 30 hari untuk Perlindungan RDS untuk aktivitas data.
- Anda dapat memilih untuk menonaktifkan pemantauan aktivitas data Perlindungan RDS atau Perlindungan RDS di Wilayah mana pun kapan saja.
- Selama uji coba gratis 30 hari, Anda bisa mendapatkan perkiraan biaya penggunaan Anda di akun dan Wilayah tersebut. Setelah uji coba gratis 30 hari berakhir, Perlindungan RDS tidak dinonaktifkan secara otomatis. Akun Anda di Wilayah ini akan mulai menimbulkan biaya penggunaan. Untuk informasi selengkapnya, lihat Memantau GuardDuty Penggunaan dan Memperkirakan Biaya.

Ketika fitur Perlindungan RDS tidak diaktifkan, GuardDuty tidak mendeteksi login atau perilaku data yang anomali atau mencurigakan. Jika Anda menonaktifkan Perlindungan RDS, GuardDuty segera berhenti memantau aktivitas RDS dan tidak akan mendeteksi potensi ancaman apa pun terhadap instans basis data yang didukung atau menghasilkan jenis temuan terkait.

Untuk Wilayah AWS tempat Aurora PostgreSQL Limitless Database didukung, lihat Persyaratan untuk Aurora PostgreSQL Limitless Database.

Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung

Tabel berikut menunjukkan versi database Aurora dan Amazon RDS yang didukung untuk pemantauan aktivitas login Perlindungan RDS dan pemantauan aktivitas data. GuardDuty dapat diperluas ke database Amazon RDS tambahan di masa depan.

Mesin Amazon Aurora dan Amazon RDS DB	Pemantauan aktivitas login versi mesin yang didukung	Pemantauan aktivitas data versi mesin yang didukung
Aurora MySQL	• 2.10.2 atau yang lebih baru • 3.02.1 atau yang lebih baru • Versi utama berikutnya	Tidak didukung
Aurora PostgreSQL	• 10.23 atau yang lebih baru • 11.12 atau yang lebih baru • 12.7 atau yang lebih baru • 13.3 atau yang lebih baru • 14.3 atau yang lebih baru • 15.2 atau yang lebih baru • 16.1 atau yang lebih baru • Versi utama berikutnya	• 11.19 atau yang lebih baru • 12.14 atau yang lebih baru • 13.10 atau yang lebih baru • 14.7 atau yang lebih baru • 15.2 atau yang lebih baru • Versi utama berikutnya
RDS for PostgreSQL	• 11.17 atau yang lebih baru • 12.12 atau yang lebih baru • 13.8 atau yang lebih baru • 14.5 atau yang lebih baru • RDS untuk PostgreSQL versi 15 • RDS untuk PostgreSQL versi 16	• 11.20 atau yang lebih baru • 12.15 atau yang lebih baru • 13.11 atau yang lebih baru • 14.8 atau yang lebih baru • 15.3 atau yang lebih baru • Versi utama berikutnya

Mesin Amazon Aurora dan Amazon RDS DB	Pemantauan aktivitas login versi mesin yang didukung	Pemantauan aktivitas data versi mesin yang didukung
	• RDS untuk PostgreSQL versi 17 • RDS untuk PostgreSQL versi 18 • Versi utama berikutnya	
Basis Data Tanpa Batas Amazon Aurora PostgreSQL	• `16.4-limitless` • Versi utama berikutnya	Tidak didukung
Amazon RDS for MariaDB	• 10.6.25 atau yang lebih baru • 10.11.16 atau yang lebih baru • 11.4.10 atau yang lebih baru • 11.8.6 atau yang lebih baru • Versi utama berikutnya	Tidak didukung
Amazon RDS for MySQL	• 8.0.45 atau yang lebih baru • 8.4.8 atau yang lebih baru • Versi utama berikutnya	Tidak didukung

Aktivitas login RDS

Saat Anda mengaktifkan fitur Perlindungan RDS, GuardDuty secara otomatis mulai memantau aktivitas login RDS untuk database Anda, langsung dari layanan Aurora dan Amazon RDS. Aktivitas login RDS menangkap upaya login yang berhasil dan gagal yang dilakukan ke lingkungan Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung Anda AWS . Jika ada indikasi perilaku login anomali, GuardDuty buat temuan dengan detail tentang database yang berpotensi dikompromikan. Saat Anda mengaktifkan Perlindungan RDS untuk pertama kalinya atau Anda memiliki instance database yang baru dibuat, ada periode pembelajaran untuk mendasar perilaku normal. Untuk alasan ini, instance database yang baru diaktifkan atau yang baru dibuat mungkin tidak memiliki temuan login anomali terkait hingga dua minggu.

Ketika Perlindungan RDS mendeteksi potensi ancaman, seperti pola yang tidak biasa dalam serangkaian upaya login yang berhasil, gagal, atau tidak lengkap, GuardDuty menghasilkan satu atau lebih. Jenis temuan Perlindungan RDS Berdasarkan jenis temuan, mungkin termasuk rincian tentang perilaku anomali, seperti. Anomali berbasis aktivitas login RDS GuardDuty tidak membuat log aktivitas login RDS tersedia untuk Anda.

Aktivitas data RDS

Saat Anda mengaktifkan Perlindungan RDS untuk aktivitas data, GuardDuty analisis pola aktivitas database dalam basis data Aurora dan Amazon RDS yang didukung untuk mengidentifikasi potensi akses data dan ancaman manipulasi. Jika mendeteksi aktivitas data anomali, GuardDuty menghasilkan temuan dengan rincian tentang database yang berpotensi dikompromikan. Saat Anda mengaktifkan Perlindungan RDS untuk aktivitas data untuk pertama kalinya, atau saat Anda membuat instance database baru, ada periode pembelajaran hingga dua minggu untuk menetapkan dasar perilaku normal. Selama waktu ini Anda mungkin tidak memiliki temuan aktivitas data anomali terkait.

Ketika Perlindungan RDS untuk aktivitas data mendeteksi potensi ancaman, GuardDuty menghasilkan satu atau lebih. Jenis temuan Perlindungan RDS Contohnya termasuk aktor yang membaca baris secara signifikan lebih banyak daripada yang normal untuk database atau pengguna tersebut, menghapus atau menjatuhkan data, atau mengakses database Anda dari alamat IP berbahaya atau Tor yang diketahui. Tergantung pada jenis temuan, temuan tersebut dapat mencakup detail tentang perilaku anomali, seperti. Anomali berbasis aktivitas data RDS GuardDuty tidak membuat log aktivitas data RDS tersedia untuk Anda.

Mengaktifkan Perlindungan RDS di lingkungan multi-akun

Dalam lingkungan multi-akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengaktifkan atau menonaktifkan fitur Perlindungan RDS, termasuk aktivitas data RDS yang memantau konfigurasi tambahan, untuk akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan ini dapat memilih untuk mengaktifkan pemantauan aktivitas login RDS secara otomatis dan pemantauan aktivitas data RDS untuk semua akun baru saat mereka bergabung dengan organisasi. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat. Mengelola beberapa akun

Mengaktifkan Perlindungan RDS untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan RDS, termasuk aktivitas data RDS yang memantau konfigurasi tambahan, untuk akun administrator yang didelegasikan GuardDuty .

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Paket Perlindungan.
3. Pilih Konfigurasikan semua enablements.
4. Di bawah Perlindungan RDS, cari entri Pemantauan Aktivitas Login RDS dan Pemantauan Aktivitas Data RDS.
5. Di kolom Akun ini, pilih Diaktifkan untuk setiap entri yang ingin Anda aktifkan, atau Tidak diaktifkan untuk menonaktifkannya.

> **Note**
>
> RDS Login Activity Monitoring harus diaktifkan sebelum Anda dapat mengaktifkan RDS Data Activity Monitoring.

API/CLI

Jalankan operasi updateDetectorAPI menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek `name` sebagai `RDS_LOGIN_EVENTS` dan `status` sebagai`ENABLED`. Untuk juga mengaktifkan pemantauan aktivitas data RDS, teruskan `RDS_DATA_RISK` sebagai bagian `name` bawah `AdditionalConfiguration` dengan `status` set ke`ENABLED`.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan ID detektor akun Anda dan *`us-east-1`* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut memungkinkan pemantauan aktivitas login RDS pada akun administrator yang didelegasikan, dan digunakan `AdditionalConfiguration` untuk juga mengaktifkan pemantauan aktivitas data RDS:

```
aws guardduty update-detector \
    --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
    --region us-east-1 \
    --features '[
        {
            "Name": "RDS_LOGIN_EVENTS",
            "Status": "ENABLED",
            "AdditionalConfiguration": [
                {
                    "Name": "RDS_DATA_RISK",
                    "Status": "ENABLED"
                }
            ]
        }
    ]'
```

Auto-enable Perlindungan RDS untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan fitur Perlindungan RDS, termasuk aktivitas data RDS yang memantau konfigurasi tambahan, untuk semua akun anggota. Ini termasuk akun anggota yang ada dan akun baru yang bergabung dengan organisasi.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensil akun GuardDuty administrator yang didelegasikan.
2. Di panel navigasi, pilih Paket Perlindungan.
3. Pilih Konfigurasikan semua enablements.
4. Di bawah Perlindungan RDS, pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan Perlindungan RDS untuk akun yang ada dan baru di organisasi.
5. Untuk juga mengaktifkan pemantauan aktivitas data RDS untuk setiap akun, perluas Konfigurasi tambahan dan pilih Aktifkan untuk semua akun untuk Pemantauan Aktivitas Data RDS.
6. Pilih Simpan semua, lalu pilih Konfirmasi dan simpan.

> **Note**
>
> Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

API/CLI

Untuk mengaktifkan Perlindungan RDS untuk semua akun anggota di organisasi Anda, termasuk anggota yang sudah ada dan akun baru yang bergabung nanti, jalankan operasi UpdateOrganizationConfigurationAPI menggunakan akun Anda sendiri. *detector ID* Setel `AutoEnable` ke `ALL` untuk `RDS_LOGIN_EVENTS` fitur tersebut, dan teruskan `AdditionalConfiguration` dengan `RDS_DATA_RISK` `AutoEnable` disetel `ALL` ke juga mengaktifkan pemantauan aktivitas data RDS secara otomatis.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut mengaktifkan otomatis keduanya `RDS_LOGIN_EVENTS` dan `RDS_DATA_RISK` untuk setiap akun anggota di organisasi:

```
aws guardduty update-organization-configuration \
    --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
    --region us-east-1 \
    --auto-enable-organization-members ALL \
    --features '[
        {
            "Name": "RDS_LOGIN_EVENTS",
            "AutoEnable": "ALL",
            "AdditionalConfiguration": [
                {
                    "Name": "RDS_DATA_RISK",
                    "AutoEnable": "ALL"
                }
            ]
        }
```

```
]'
```

> **Note**
>
> Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Aktifkan Perlindungan RDS untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan RDS, termasuk konfigurasi tambahan pemantauan aktivitas data RDS, untuk semua akun anggota aktif yang ada di organisasi Anda. Akun anggota yang sudah GuardDuty diaktifkan, disebut sebagai anggota aktif yang ada.

> **Note**
>
> RDS Login Activity Monitoring harus diaktifkan pada akun anggota sebelum Anda dapat mengaktifkan RDS Data Activity Monitoring pada akun tersebut.

Console

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.
2. Di panel navigasi, pilih Akun.
3. Pada halaman Akun, pilih akun anggota aktif yang sudah ada yang ingin Anda aktifkan. Untuk memilih setiap akun, gunakan kotak centang di header tabel.
4. Dari menu tarik-turun Edit Rencana Perlindungan, pilih Aktivitas Login RDS, lalu pilih Aktifkan.
5. Untuk juga mengaktifkan pemantauan aktivitas data RDS pada akun yang dipilih, buka menu tarik-turun Edit Rencana Perlindungan lagi, pilih Aktivitas Data RDS, lalu pilih Aktifkan. Pemantauan Aktivitas Login RDS harus sudah diaktifkan pada setiap akun yang dipilih.

API/CLI

Jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri*detector ID*. `RDS_DATA_RISK`AdditionalConfigurationTeruskan `RDS_LOGIN_EVENTS` fitur untuk juga mengontrol pemantauan aktivitas data RDS.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut memungkinkan pemantauan aktivitas login RDS pada akun anggota aktif yang ada, dan digunakan `AdditionalConfiguration` untuk juga mengaktifkan pemantauan aktivitas data RDS:

```
aws guardduty update-member-detectors \
    --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
    --region us-east-1 \
    --account-ids 111122223333 \
    --features '[
        {
            "Name": "RDS_LOGIN_EVENTS",
            "Status": "ENABLED",
            "AdditionalConfiguration": [
                {
                    "Name": "RDS_DATA_RISK",
                    "Status": "ENABLED"
                }
            ]
        }
    ]'
```

Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Auto-enable Perlindungan RDS untuk akun anggota baru

Pilih metode akses pilihan Anda untuk mengaktifkan pemantauan aktivitas login RDS dan pemantauan aktivitas data RDS untuk akun baru yang bergabung dengan organisasi Anda.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensil akun GuardDuty administrator yang didelegasikan.
2. Di panel navigasi, pilih Paket Perlindungan.
3. Pilih Konfigurasikan semua enablements.
4. Pilih Konfigurasikan akun secara manual.
5. Di bawah Perlindungan RDS, pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, Perlindungan RDS akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
6. Untuk juga mengaktifkan pemantauan aktivitas data RDS secara otomatis untuk akun baru, perluas Konfigurasi tambahan dan pilih Aktifkan secara otomatis untuk akun anggota baru untuk Pemantauan Aktivitas Data RDS.
7. Pilih Simpan.

API/CLI

Untuk mengaktifkan Perlindungan RDS secara otomatis untuk akun baru yang bergabung dengan organisasi Anda, jalankan operasi UpdateOrganizationConfigurationAPI menggunakan akun Anda sendiri. *`detector ID`* Setel `AutoEnable` ke `NEW` untuk `RDS_LOGIN_EVENTS` fitur tersebut, dan teruskan `AdditionalConfiguration` dengan `RDS_DATA_RISK` `AutoEnable` disetel `NEW` ke juga mengaktifkan pemantauan aktivitas data RDS secara otomatis. Untuk menghentikan mengaktifkan fitur secara otomatis untuk akun baru, tetapkan `AutoEnable` nilainya ke. `NONE`

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan ID detektor akun Anda dan *`us-east-1`* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut mengaktifkan otomatis keduanya `RDS_LOGIN_EVENTS` dan `RDS_DATA_RISK` untuk akun baru yang bergabung dengan organisasi:

```
aws guardduty update-organization-configuration \
    --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
    --region us-east-1 \
    --auto-enable-organization-members NEW \
    --features '[
        {
            "Name": "RDS_LOGIN_EVENTS",
            "AutoEnable": "NEW",
            "AdditionalConfiguration": [
                {
                    "Name": "RDS_DATA_RISK",
                    "AutoEnable": "NEW"
                }
            ]
        }
    ]'
```

Aktifkan Perlindungan RDS secara selektif untuk akun anggota

Pilih metode akses pilihan Anda untuk secara selektif mengaktifkan pemantauan aktivitas login RDS dan aktivitas data RDS untuk akun anggota.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensil akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.

   Pada halaman Akun, tinjau aktivitas login RDS dan kolom aktivitas data RDS untuk status akun anggota Anda.

3. Untuk mengaktifkan atau menonaktifkan aktivitas login RDS secara selektif

   Pilih akun yang ingin Anda konfigurasikan Perlindungan RDS. Anda dapat memilih beberapa akun sekaligus. Di menu tarik-turun Edit Rencana Perlindungan, pilih Aktivitas Login RDS, lalu pilih opsi yang sesuai.

4. Untuk mengaktifkan atau menonaktifkan aktivitas data RDS secara selektif

   Pilih akun yang ingin Anda konfigurasikan pemantauan aktivitas data RDS. Anda dapat memilih beberapa akun sekaligus. Di menu tarik-turun Edit Rencana Perlindungan, pilih Aktivitas Data RDS, lalu pilih opsi yang sesuai.

API/CLI

Untuk mengaktifkan atau menonaktifkan Perlindungan RDS secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectorsAPI menggunakan milik Anda sendiri. *detector ID* `RDS_DATA_RISKAdditionalConfiguration`Teruskan `RDS_LOGIN_EVENTS` fitur untuk mengontrol pemantauan aktivitas data RDS secara independen.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut memungkinkan keduanya `RDS_LOGIN_EVENTS` dan`RDS_DATA_RISK`:

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"Name":
 "RDS_LOGIN_EVENTS", "Status": "ENABLED", "AdditionalConfiguration": [{"Name":
 "RDS_DATA_RISK", "Status": "ENABLED"}]}]'
```

Untuk menjaga pemantauan aktivitas login RDS tetap aktif saat mematikan pemantauan aktivitas data RDS, setel `RDS_LOGIN_EVENTS` `Status` ke `ENABLED` dan `RDS_DATA_RISK` `Status` ke: `DISABLED`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"Name":
 "RDS_LOGIN_EVENTS", "Status": "ENABLED", "AdditionalConfiguration": [{"Name":
 "RDS_DATA_RISK", "Status": "DISABLED"}]}]'
```

> **Note**
>
> Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Mengaktifkan Perlindungan RDS untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat Mengaktifkan Perlindungan RDS di lingkungan multi-akun.

Setelah Anda mengaktifkan Perlindungan RDS, GuardDuty akan mulai memantau Aktivitas login RDS basis data yang didukung di akun Anda.

Pilih metode akses pilihan Anda untuk mengonfigurasi Perlindungan RDS untuk akun mandiri.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Paket Perlindungan.
3. Pilih Konfigurasikan semua enablements. Di bawah Perlindungan RDS, pilih Aktifkan untuk mengaktifkan Perlindungan RDS.
4. Pilih Simpan semua, lalu pilih Konfirmasi dan simpan.

API/CLI

Jalankan operasi updateDetectorAPI menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek `name` sebagai `RDS_LOGIN_EVENTS` dan `status` sebagai`ENABLED`. Untuk juga mengaktifkan pemantauan aktivitas data RDS, teruskan `RDS_DATA_RISK` sebagai bagian `name` bawah `AdditionalConfiguration` dengan `status` set ke`ENABLED`.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan ID detektor akun Anda dan *`us-east-1`* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

Contoh berikut memungkinkan keduanya `RDS_LOGIN_EVENTS` dan`RDS_DATA_RISK`:

```
aws guardduty update-detector \
    --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
    --region us-east-1 \
    --features '[
        {
            "Name": "RDS_LOGIN_EVENTS",
            "Status": "ENABLED",
            "AdditionalConfiguration": [
                {
                    "Name": "RDS_DATA_RISK",
                    "Status": "ENABLED"
                }
            ]
        }
    ]'
```

Memecahkan masalah pemantauan Perlindungan RDS

GuardDuty RDS Protection menganalisis dan memprofilkan aktivitas login RDS Anda untuk potensi ancaman akses ke. Basis data yang didukung Untuk mengumpulkan telemetri keamanan secara efektif, GuardDuty diperlukan database Anda dikonfigurasi dan beroperasi tanpa masalah. Jika database Anda salah konfigurasi atau mengalami masalah, maka pemantauan keamanan mungkin terpengaruh.

Bagian berikut menyediakan masalah umum dan langkah-langkah untuk memecahkan masalah mereka.

Penyimpanan RDS penuh

Ketika instans RDS Anda kehabisan penyimpanan, GuardDuty mungkin tidak mengumpulkan telemetri keamanan. Mencapai alokasi kapasitas penyimpanan instans DB (`storage-full`) adalah status penting, dan RDS merekomendasikan untuk segera memperbaiki masalah ini. Untuk informasi selengkapnya, lihat Melihat status instans di Panduan Pengguna Amazon RDS.

Untuk menyelesaikan `storage-full` status, Anda dapat melakukan salah satu tindakan berikut:

- Aktifkan penskalaan otomatis penyimpanan (disarankan) — Aktifkan penskalaan otomatis penyimpanan Amazon RDS untuk mengelola kapasitas penyimpanan secara otomatis dan mencegah kondisi di masa mendatang. `storage-full` Untuk informasi selengkapnya, lihat Mengelola kapasitas secara otomatis dengan penskalaan otomatis penyimpanan Amazon RDS di Panduan Pengguna Amazon RDS.
- Pantau pemanfaatan penyimpanan Anda — Periksa pemanfaatan penyimpanan Anda menggunakan salah satu metode berikut:
  - Gunakan CloudWatch metrik untuk melihat detail tentang penyimpanan. Untuk informasi selengkapnya, lihat Wawasan CloudWatch Database di Panduan CloudWatch Pengguna Amazon.
  - Lihat metrik penyimpanan dengan mengikuti langkah-langkah dalam Metrik Monitor di instans Amazon RDS di Panduan Pengguna Amazon RDS.
- Memodifikasi kapasitas penyimpanan — Untuk informasi tentang meningkatkan kapasitas penyimpanan instans Anda, lihat Meningkatkan kapasitas penyimpanan instans DB di Panduan Pengguna Amazon RDS.

Versi yang tidak didukung pada database utama untuk RDS untuk PostgreSQL

RDS untuk instance replika baca PostgreSQL memerlukan instance database utama berada pada versi database yang didukung dan berhasil direplikasi dari database utama. GuardDuty memantau instans Anda hanya ketika persyaratan ini terpenuhi.

Untuk mengatasi masalah versi yang tidak didukung, lakukan salah satu hal berikut:

- Verifikasi kompatibilitas versi database — Periksa apakah RDS utama Anda untuk database PostgreSQL menjalankan salah satu versi yang didukung. Untuk informasi selengkapnya, lihat Basis data yang didukung.
- Atasi potensi masalah replikasi — Tinjau dan selesaikan masalah replikasi apa pun antara instance primer dan replika. Untuk informasi selengkapnya tentang melakukan hal ini, lihat Bekerja dengan replika baca untuk RDS for PostgreSQL di Panduan Pengguna Amazon RDS.

Pertimbangan keamanan tambahan

Jika organisasi Anda memiliki persyaratan kepatuhan yang ketat, sebaiknya implementasikan audit basis data selain menggunakan Perlindungan RDS. Untuk informasi selengkapnya tentang tanggung

jawab keamanan dan model tanggung jawab bersama, lihat Keamanan di Amazon RDS di Panduan Pengguna Amazon RDS.

GuardDuty Perlindungan Lambda

> **Note**
>
> Anda dapat mengonfigurasi Perlindungan Lambda bersama dengan semua paket perlindungan lainnya dari satu halaman di GuardDuty konsol. Untuk informasi selengkapnya, lihat Mengkonfigurasi rencana perlindungan.

Lambda Protection membantu Anda mengidentifikasi potensi ancaman keamanan saat suatu AWS Lambdafungsi dipanggil di lingkungan Anda. AWS Saat Anda mengaktifkan Perlindungan Lambda, GuardDuty mulai memantau log aktivitas jaringan Lambda. Ini termasuk Log Alur VPC dari semua fungsi Lambda untuk akun Anda (termasuk log yang tidak menggunakan jaringan VPC) dan log yang dihasilkan saat fungsi Lambda dipanggil. Ketika GuardDuty mengidentifikasi lalu lintas jaringan yang mencurigakan yang menunjukkan adanya potongan kode yang berpotensi berbahaya dalam fungsi Lambda Anda, GuardDuty menghasilkan satu atau lebih. Jenis temuan Perlindungan Lambda

Uji coba gratis 30 hari

Daftar berikut menjelaskan cara kerja uji coba gratis 30 hari untuk akun Anda:

- Saat Anda mengaktifkan GuardDuty di Wilayah baru untuk pertama kalinya, Anda mendapatkan uji coba gratis 30 hari. Akun AWS Dalam hal ini, juga GuardDuty akan mengaktifkan Perlindungan Lambda, yang termasuk dalam uji coba gratis.
- Ketika Anda sudah menggunakan GuardDuty dan memutuskan untuk mengaktifkan Perlindungan Lambda untuk pertama kalinya, akun Anda di Wilayah ini akan mendapatkan uji coba gratis 30 hari untuk Perlindungan Lambda.
- Anda dapat memilih untuk menonaktifkan Perlindungan Lambda di Wilayah mana pun kapan saja.
- Selama uji coba gratis 30 hari, Anda bisa mendapatkan perkiraan biaya penggunaan Anda di akun dan Wilayah tersebut. Setelah uji coba gratis 30 hari berakhir, Perlindungan Lambda tidak dinonaktifkan secara otomatis. Akun Anda di Wilayah ini akan mulai menimbulkan biaya penggunaan. Untuk informasi selengkapnya, lihat Memantau GuardDuty Penggunaan dan Memperkirakan Biaya.

Log aktivitas jaringan Lambda dapat berubah, termasuk ekspansi ke aktivitas jaringan lain seperti data kueri DNS yang dihasilkan dengan menjalankan fungsi Lambda. Ekspansi ke bentuk lain dari

pemantauan aktivitas jaringan akan meningkatkan volume data yang GuardDuty akan diproses untuk Perlindungan Lambda. Ini akan berdampak langsung pada biaya penggunaan Perlindungan Lambda. Setiap kali GuardDuty mulai memantau log aktivitas jaringan tambahan, itu akan memberikan pemberitahuan ke akun yang telah mengaktifkan Perlindungan Lambda, setidaknya 30 hari sebelum rilis.

> **Note**
>
> Pemantauan Aktivitas Jaringan Lambda tidak menyertakan log untuk fungsi Lambda @Edge.

Pemantauan Aktivitas Jaringan Lambda

Saat Anda mengaktifkan Perlindungan Lambda, memantau log aktivitas jaringan GuardDuty Lambda yang dihasilkan saat fungsi Lambda, yang terkait dengan akun Anda, dipanggil. Ini membantu Anda mendeteksi potensi ancaman keamanan terhadap fungsi Lambda. Untuk fungsi Lambda yang dikonfigurasi untuk menggunakan jaringan VPC, Anda tidak perlu mengaktifkan log aliran VPC untuk antarmuka jaringan elastis (ENI) yang dibuat oleh Lambda untuk. GuardDuty GuardDuty hanya mengenakan biaya untuk jumlah data log aktivitas jaringan Lambda yang diproses (dalam GB) untuk menghasilkan temuan. GuardDuty mengoptimalkan biaya dengan menerapkan filter pintar dan menganalisis subset log aktivitas jaringan Lambda yang relevan dengan deteksi ancaman.

GuardDuty tidak mengelola log aktivitas jaringan Lambda Anda (termasuk log aliran VPC dan non-VPC), atau membuatnya dapat diakses di akun Anda.

Mengaktifkan Perlindungan Lambda di lingkungan multi-akun

Dalam lingkungan multi-akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengaktifkan atau menonaktifkan Perlindungan Lambda untuk akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan dapat memilih untuk mengaktifkan secara otomatis Pemantauan Aktivitas Jaringan Lambda untuk semua akun baru saat mereka bergabung dengan organisasi. Untuk informasi selengkapnya tentang lingkungan beberapa akun, lihat Mengelola beberapa akun di Amazon. GuardDuty

Mengaktifkan Perlindungan Lambda untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun administrator yang didelegasikan GuardDuty .

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, di bawah Pengaturan, pilih Perlindungan Lambda.
3. Pada halaman Perlindungan Lambda, pilih Edit.
4. Lakukan salah satu tindakan berikut:

   Menggunakan Aktifkan untuk semua akun

   - Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
   - Pilih Simpan.

   Menggunakan Konfigurasi akun secara manual

   - Untuk mengaktifkan paket perlindungan hanya untuk akun akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
   - Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
   - Pilih Simpan.

API/CLI

Jalankan operasi updateDetectorAPI menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek `name` sebagai `LAMBDA_NETWORK_LOGS` dan `status` sebagai`ENABLED`.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Jalankan perintah berikut, dan ganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan ID detektor akun Anda dan *`us-east-1`* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Auto-enable Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan fitur Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota. Ini termasuk akun anggota yang ada dan akun baru yang bergabung dengan organisasi.

Console

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.
2. Lakukan salah satu tindakan berikut:

   Menggunakan halaman Rencana Perlindungan

   1. Di panel navigasi, pilih Paket Perlindungan.
   2. Pilih Konfigurasikan semua enablements.
   3. Di bawah Perlindungan Lambda, pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan Pemantauan Aktivitas Jaringan Lambda untuk akun yang ada dan baru di organisasi.
   4. Pilih Simpan semua, lalu pilih Konfirmasi dan simpan.

   > **Note**
   >
   > Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

   Menggunakan halaman Akun

   1. Di panel navigasi, pilih Akun.

2. Pada halaman Akun, pilih Auto-enablepreferensi sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah Pemantauan Aktivitas Jaringan Lambda.

> **Note**
>
> Secara default, tindakan ini secara otomatis mengaktifkan opsi Auto-enable GuardDuty untuk akun anggota baru.

4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun, lihatAktifkan atau nonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota.

API/CLI

Untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota Anda, jalankan operasi API menggunakan updateMemberDetectorsmilik Anda sendiri. *`detector ID`*

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Jalankan perintah berikut, dan ganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan ID detektor akun Anda dan *`us-east-1`* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --region us-east-1--features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota aktif yang ada di organisasi.

Console

Untuk mengonfigurasi Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota aktif yang ada

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.
2. Di panel navigasi, pilih Paket Perlindungan.
3. Pilih Konfigurasikan semua enablements. Di bawah Perlindungan Lambda, Anda dapat melihat status konfigurasi saat ini. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
5. Pilih Konfirmasi.

API/CLI

Untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota Anda, jalankan operasi API menggunakan updateMemberDetectorsmilik Anda sendiri. *detector ID*

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Jalankan perintah berikut, dan ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Auto-enable Pemantauan Aktivitas Jaringan Lambda untuk akun anggota baru

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun baru yang bergabung dengan organisasi Anda.

Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun anggota baru di organisasi, menggunakan halaman Perlindungan Lambda atau Akun.

Untuk mengaktifkan secara otomatis Pemantauan Aktivitas Jaringan Lambda untuk akun anggota baru

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.
2. Lakukan salah satu tindakan berikut:
   - Menggunakan halaman Paket Perlindungan:
     1. Di panel navigasi, pilih Paket Perlindungan.
     2. Pilih Konfigurasikan semua enablements.
     3. Pilih Konfigurasikan akun secara manual.
     4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, Perlindungan Lambda akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
     5. Pilih Simpan.
   - Menggunakan halaman Akun:
     1. Di panel navigasi, pilih Akun.
     2. Pada halaman Akun, pilih Auto-enablepreferensi.

3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Pemantauan Aktivitas Jaringan Lambda.
4. Pilih Simpan.

API/CLI

Untuk mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun anggota baru, jalankan operasi UpdateOrganizationConfigurationAPI menggunakan milik Anda sendiri. *`detector ID`*

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk satu akun anggota. Ganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan ID detektor akun Anda dan *`us-east-1`* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda. Jika Anda tidak ingin mengaktifkannya untuk semua akun baru yang bergabung dengan organisasi, setel `AutoEnable` ke`NONE`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features
 '[{"Name": "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan atau nonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, di bagian Pengaturan, pilih Akun.

   Pada halaman Akun, tinjau kolom Pemantauan Aktivitas Jaringan Lambda. Ini menunjukkan apakah Pemantauan Aktivitas Jaringan Lambda diaktifkan atau tidak.
3. Pilih akun yang ingin Anda konfigurasikan Perlindungan Lambda. Anda dapat memilih beberapa akun sekaligus.
4. Dari menu tarik-turun Edit Rencana Perlindungan, pilih Pemantauan Aktivitas Jaringan Lambda, lalu pilih tindakan yang sesuai.

API/CLI

Panggil updateMemberDetectorsAPI menggunakan milik Anda sendiri*detector ID*.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar ID akun yang dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Mengaktifkan Perlindungan Lambda untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat Mengaktifkan Perlindungan Lambda di lingkungan multi-akun.

Setelah Anda mengaktifkan Perlindungan Lambda, GuardDuty akan mulai memantau Pemantauan Aktivitas Jaringan Lambda di akun Anda.

Pilih metode akses pilihan Anda untuk mengonfigurasi Perlindungan Lambda untuk akun mandiri.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, di bawah Pengaturan, pilih Perlindungan Lambda.
3. Halaman Perlindungan Lambda menunjukkan status akun Anda saat ini. Pilih Aktifkan untuk mengaktifkan Perlindungan Lambda di akun Anda.
4. Pilih Konfirmasi untuk menyimpan pilihan Anda.

API/CLI

Jalankan operasi updateDetectorAPI menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek `name` sebagai `LAMBDA_NETWORK_LOGS` dan `status` sebagai`ENABLED`.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Jalankan perintah berikut, dan ganti *`12abc34d567e8fa901bc2d34e56789f0`* dengan ID detektor akun Anda dan *`us-east-1`* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" :
 "ENABLED"}]'
```

GuardDuty Investigasi (Pratinjau)

GuardDuty Investigasi memberikan analisis AI-powered keamanan dari GuardDuty temuan dan akun Anda. Saat Anda membuat investigasi, periksa GuardDuty konteks pencarian, aktivitas terkait dari 90 hari terakhir, sumber daya yang terpengaruh, intelijen ancaman, dan indikator ancaman menggunakan grafik pengetahuan. Setiap investigasi memberikan penilaian disposisi ancaman dengan penilaian kepercayaan, klasifikasi teknik MITRE ATT&CK®, bukti pendukung, dan rekomendasi yang dapat ditindaklanjuti.

Setiap penyelidikan menghasilkan wawasan berikut:

- Tingkat risiko — Penilaian risiko keseluruhan: Info, Rendah, Sedang, Tinggi, atau Kritis.
- Key akinan — Tingkat kepercayaan penilaian: Tidak Diketahui, Rendah, Sedang, atau Tinggi.
- Ringkasan — Deskripsi temuan investigasi dan pengamatan utama.
- Rincian In vestigasi — Informasi tambahan dan konteks yang terkait dengan penyelidikan.
- Tindakan yang Direkomendasikan — Tindakan terperinci, termasuk perintah CLI, yang dapat Anda lakukan untuk mengatasi masalah yang teridentifikasi.

> **Note**
>
> GuardDuty Investigasi hanya tersedia di 10 Wil AWS ayah komersial berikut: AS Timur (Virginia Utara), AS Timur (Ohio), AS Barat (Oregon), Kanada (Tengah), Eropa (Frankfurt), Eropa (Irlandia), Eropa (London), Eropa (Paris), Eropa (Stockholm), dan Asia Pasifik (Tokyo).

Jenis analisis

GuardDuty Investigasi mendukung tiga jenis analisis berikut:

- Analisis menemukan — Menganalisis GuardDuty temuan tertentu, ketika Anda menentukan ID temuan (heksadesimal 32 karakter). Untuk pratinjau, GuardDuty Investigasi mendukung semua temuan Extended Threat Detection (XTD) dan memilih temuan dari rencana dasar, S3, dan Runtime.
- Analisis akun — Menganalisis postur ancaman AWS akun, saat Anda memberikan ID AWS akun 12 digit.

- Analisis organisasi — Menganalisis postur ancaman organisasi Anda.

Cross-Region kesimpulan

GuardDuty Investigasi memanfaatkan Layanan Cross-Region Inferensi (CRIS), yang secara otomatis memilih yang optimal Wilayah AWS dalam geografi Anda untuk memproses analisis investigasi dan menghasilkan laporan investigasi. Ini memaksimalkan sumber daya komputasi yang tersedia, ketersediaan model, dan memberikan pengalaman pelanggan terbaik.

Data Anda tetap disimpan hanya di Wilayah tempat permintaan investigasi berasal. Namun, data investigasi dan hasil ringkasan dapat diproses di luar Wilayah tersebut. Semua data dikirim terenkripsi di seluruh jaringan aman Amazon.

GuardDuty Investigasi secara aman merutekan permintaan inferensi Anda ke sumber daya komputasi yang tersedia dalam wilayah geografis tempat permintaan berasal, seperti yang ditunjukkan pada tabel berikut.

Cross-Region perutean inferensi

Geografi yang didukung	GuardDuty Wilayah	Wilayah Inferensi
Amerika Serikat	AS Timur (Virginia Utara)	AS Timur (Virginia Utara), AS Timur (Ohio), AS Barat (Oregon)
Amerika Serikat	AS Timur (Ohio)	AS Timur (Virginia Utara), AS Timur (Ohio), AS Barat (Oregon)
Amerika Serikat	AS Barat (Oregon)	AS Timur (Virginia Utara), AS Timur (Ohio), AS Barat (Oregon)
Amerika Serikat	Kanada (Pusat)	Kanada (Tengah), AS Timur (Virginia Utara), AS Timur (Ohio), AS Barat (Oregon)
Eropa	Eropa (Frankfurt)	Eropa (Frankfurt), Eropa (Stockholm), Eropa (Milan), Eropa (Spanyol), Eropa (Irlandia), Eropa (Paris)
Eropa	Eropa (Irlandia)	Eropa (Frankfurt), Eropa (Stockholm), Eropa (Milan), Eropa (Spanyol), Eropa (Irlandia), Eropa (Paris)

Geografi yang didukung	GuardDuty Wilayah	Wilayah Inferensi
Eropa	Eropa (London)	Eropa (Frankfurt), Eropa (Stockholm), Eropa (Milan), Eropa (Spanyol), Eropa (Irlandia), Eropa (London), Eropa (Paris)
Eropa	Eropa (Paris)	Eropa (Frankfurt), Eropa (Stockholm), Eropa (Milan), Eropa (Spanyol), Eropa (Irlandia), Eropa (Paris)
Eropa	Eropa (Stockholm)	Eropa (Frankfurt), Eropa (Stockholm), Eropa (Milan), Eropa (Spanyol), Eropa (Irlandia), Eropa (Paris)
Jepang	Asia Pasifik (Tokyo)	Asia Pasifik (Tokyo), Asia Pasifik (Osaka)

Prasyarat

Sebelum Anda dapat menggunakan In GuardDuty vestigasi, pastikan bahwa prasyarat berikut terpenuhi:

- Anda harus memiliki GuardDuty detektor aktif di Wilayah AWS tempat Anda ingin membuat penyelidikan. Untuk informasi selengkapnya tentang mengaktifkan GuardDuty, lihatMemulai dengan GuardDuty.
- Anda harus mengaktifkan fitur In GuardDuty vestigasi pada detektor Anda.

  Console

  1. Buka GuardDuty konsol.
  2. Pada panel navigasi, silakan pilih Pengaturan.
  3. Di bawah Investigasi yang didukung AI - Pratinjau, pilih Aktifkan.

  API/CLI

  Panggil UpdateDetector API dan aktifkan `AI_ANALYST` fitur pada detektor Anda.

```
aws guardduty update-detector \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --features '[{"Name": "AI_ANALYST", "Status": "ENABLED"}]'
```

- Identitas IAM Anda harus memiliki izin yang diperlukan untuk melakukan tindakan investigasi. Tindakan IAM berikut diperlukan:
  - `guardduty:CreateInvestigation`— Diperlukan untuk membuat penyelidikan baru.
  - `guardduty:GetInvestigation`— Diperlukan untuk mengambil hasil investigasi.
  - `guardduty:ListInvestigations`- Diperlukan untuk membuat daftar investigasi untuk detektor.

Contoh kebijakan IAM berikut memberikan izin untuk menggunakan semua tindakan Investig GuardDuty asi:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateInvestigation",
                "guardduty:GetInvestigation",
                "guardduty:ListInvestigations"
            ],
            "Resource": "arn:aws:guardduty:us-
west-2:123456789012:detector/2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7"
        }
    ]
}
```

Model akses untuk akun administrator dan anggota

Aturan akses berikut berlaku untuk GuardDuty Investigasi tergantung pada apakah Anda menggunakan akun administrator atau akun anggota:

- Akun administrator — Dapat membuat, mendapatkan, dan membuat daftar investigasi untuk diri mereka sendiri dan akun anggota mereka.
- Akun anggota — Hanya dapat mendapatkan dan membuat daftar investigasi untuk akun mereka sendiri. Akun anggota tidak dapat melakukan investigasi dan tidak dapat mengakses investigasi milik akun lain atau akun administrator.

Membuat investigasi

Anda dapat membuat penyelidikan untuk menganalisis GuardDuty temuan dan akun di AWS lingkungan Anda. Investigasi berjalan secara asinkron di latar belakang. Setelah Anda membuat investigasi, gunakan ID investigasi untuk memeriksa statusnya dan mengambil hasilnya.

> **Important**
>
> Selama pratinjau, Anda dapat memulai hingga 10 investigasi per akun per hari, dengan batas total 100 investigasi per akun. Investigasi yang gagal tidak diperhitungkan dalam kuota ini. Jika Anda menggunakan API/CLI, prompt pemicu bisa mencapai 2.048 karakter.

Pilih metode akses pilihan Anda untuk membuat penyelidikan.

Console

1. Buka GuardDuty konsol dan arahkan ke Investigasi di navigasi kiri.
2. Pilih Mem ulai investigasi.
3. Pilih ruang lingkup investigasi:
   - Temuan spesifik — Masukkan ID temuan yang ingin Anda analisis.
   - Akun saya (mandiri saja) - Tidak diperlukan input tambahan. GuardDuty akan menganalisis akun Anda.
   - Akun tertentu (hanya administrator) — Masukkan ID AWS akun 12 digit.
   - Semua akun dalam organisasi (hanya administrator) - Tidak diperlukan input tambahan.
4. Pilih Memulai investig asi untuk memulai analisis.

API/CLI

Jalankan operasi CreateInvestigation API untuk memulai penyelidikan baru. Anda harus memberikan ID detektor dan prompt pemicu yang menjelaskan apa yang harus diselidiki.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

```
aws guardduty create-investigation \
```

```
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --trigger-prompt "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in
 account 123456789012"
```

Pada perintah sebelumnya, ganti *detector-id* dengan ID detektor Anda sendiri dan *trigger-prompt* dengan deskripsi tentang apa yang ingin Anda selidiki.

Anda dapat secara opsional menyertakan `--client-token` parameter untuk idempotensi. Jika Anda mencoba kembali permintaan dengan token klien yang sama, GuardDuty mengembalikan investigasi yang ada alih-alih membuat duplikat.

Contoh output:

```
{
    "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890"
}
```

Persyaratan prompt pemicu

Prompt pemicu harus menjelaskan apa yang harus diselidiki. GuardDuty menentukan jenis analisis berdasarkan konten prompt Anda:

- Analisis menemukan - Sertakan tepat satu ID temuan (string heksadesimal 32 karakter) dalam prompt. Temuan harus ada dan milik akun penelepon atau akun anggota. Anda tidak dapat menyertakan beberapa ID pencarian dalam satu prompt.
- Analisis akun — Sertakan tepat satu ID AWS akun 12 digit dalam prompt. Penelepon harus administrator akun itu. Anda tidak dapat menyertakan beberapa ID akun dalam satu prompt.
- Analisis organisasi — Jelaskan masalah keamanan di seluruh organisasi dalam prompt Anda. Investigasi menganalisis sinyal di seluruh organisasi.

GuardDuty menggunakan AI untuk menafsirkan prompt bentuk bebas Anda dan menentukan ruang lingkup analisis yang sesuai. Jika Anda menyertakan ID temuan, itu melakukan analisis pencarian. Jika Anda menyertakan ID akun, itu akan melakukan analisis akun. Jika prompt Anda menjelaskan masalah di seluruh organisasi, ia melakukan analisis organisasi. Jika prompt tidak cocok dengan jenis analisis tertentu, penyelidikan secara default menganalisis akun penelepon itu sendiri.

Berikut ini adalah contoh prompt pemicu untuk setiap jenis analisis:

- Menemukan analisis — `"Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in account 123456789012"`
- Analisis akun - `"Analyze findings in account with id 123456789012"`
- Analisis organisasi — `"Analyze findings in my organization"`

Membuat investigasi untuk akun anggota

Jika Anda adalah akun administrator, Anda dapat membuat penyelidikan untuk akun anggota dengan menyertakan ID akun anggota dalam prompt pemicu. Gunakan ID detektor akun administrator dalam perintah. Hasil investigasi akan berisi temuan dari akun anggota yang ditentukan.

```
aws guardduty create-investigation \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --trigger-prompt "Analyze findings in account with id 111122223333"
```

Pada perintah sebelumnya, ganti *detector-id* dengan ID detektor akun administrator Anda. ID akun 12 digit dalam prompt pemicu mengidentifikasi akun anggota untuk diselidiki.

Melihat hasil investigasi

Setelah membuat investigasi, Anda dapat mengambil hasil termasuk ringkasan, detail investigasi, tingkat kepercayaan, dan rekomendasi. Investigasi dapat memiliki salah satu status berikut:

- BERJALAN — Investigasi masih berlangsung.
- SELES AI — Investigasi selesai dengan sukses dan hasilnya tersedia.
- GAG AL — Investigasi mengalami kesalahan. Periksa bidang kesalahan untuk detailnya.

Pilih metode akses pilihan Anda untuk melihat hasil investigasi.

AI-generated analisis dan rekomendasi mungkin mengandung kesalahan atau penilaian yang tidak lengkap. Tinjauan manusia direkomendasikan.

Console

1. Buka GuardDuty konsol dan arahkan ke Investigasi di navigasi kiri.
2. Dalam tabel investigasi, temukan investigasi lengkap yang ingin Anda tinjau.

3. Pilih tautan judul investigasi untuk membuka halaman detail.

> **Note**
>
> Judul investigasi hanya dapat diklik ketika status Sel esai.

API/CLI

Jalankan operasi GetInvestigation API untuk mengambil rincian lengkap dari penyelidikan yang telah selesai.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

```
aws guardduty get-investigation \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --investigation-id a1b2c3d4-5678-90ab-cdef-ef1234567890
```

Contoh keluaran untuk penyelidikan yang selesai:

```
{
    "Investigation": {
        "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890",
        "Status": "COMPLETED",
        "TriggerPrompt": "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in
 account 123456789012",
        "TriggeredBy": "123456789012",
        "RiskLevel": "Critical",
        "Risk": "Detection logic is valid but no live resources are compromised.",
        "Confidence": "High",
        "Summary": "{\"keyObservations\":{\"title\":\"...\",\"narrative\":\"...\",
\"observations\":[...]},\"countermeasures\":[...],\"threatAssessment\":{...}}",
        "Cloud": {
            "Provider": "AWS",
            "Region": "us-east-1",
            "Account": "123456789012"
        },
        "Metadata": {
            "Product": {
                "Name": "Amazon GuardDuty AI Analyst",
```

```
                "Feature": "Investigation"
            },
            "Version": "1.0.0"
        },
        "StartTime": 1705319400.0,
        "EndTime": 1705319700.0
    }
}
```

Bid `Summary` ang berisi string JSON dengan hasil investigasi lengkap, termasuk pengamatan utama, penanggulangan dengan perintah CLI, dan penilaian ancaman MITRE ATT&CK®.

Menafsirkan hasil investigasi

Tabel berikut menjelaskan tingkat risiko yang dapat dikembalikan oleh investigasi:

Tingkat risiko investigasi

Tingkat risiko	Deskripsi
Info	Temuan informasi tanpa risiko teridentifikasi terhadap lingkungan.
Rendah	Risiko kecil yang tidak mungkin memerlukan tindakan segera.
Sedang	Risiko sedang yang harus Anda tinjau dan mungkin memerlukan perbaikan.
Tinggi	Risiko signifikan yang membutuhkan penyelidikan dan remediasi yang cepat.
Kritis	Risiko berat yang membutuhkan tindakan segera untuk mencegah kompromi lebih lanjut.

Tabel berikut menjelaskan tingkat kepercayaan:

Tingkat kepercayaan investigasi

Tingkat kepercayaan	Deskripsi
Tidak Diketahui	Data tidak mencukupi untuk menentukan kepercayaan dalam penilaian.

Tingkat kepercayaan	Deskripsi
Rendah	Bukti terbatas mendukung penilaian.
Sedang	Bukti moderat mendukung penilaian.
Tinggi	Bukti kuat mendukung penilaian.

Investigasi daftar

Anda dapat membuat daftar semua investigasi untuk detektor, dengan penyortiran dan paginasi opsional. Ini membantu Anda meninjau dan melacak status beberapa penyelidikan.

Pilih metode akses pilihan Anda untuk membuat daftar investigasi.

Console

1. Buka GuardDuty konsol dan arahkan ke Investigasi di navigasi kiri.
2. Tabel investigasi menampilkan semua investigasi untuk detektor saat ini dengan status, tingkat risiko, dan cap waktu.

API/CLI

Jalankan operasi ListInvestigations API untuk mencantumkan ringkasan investigasi untuk detektor.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

```
aws guardduty list-investigations \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --max-results 10
```

Anda dapat mengurutkan hasil dengan menentukan `--sort-criteria` parameter. Contoh berikut mencantumkan investigasi yang diurutkan berdasarkan waktu mulai dalam urutan menurun:

```
aws guardduty list-investigations \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
```

```
    --sort-criteria '{"attributeName": "START_TIME", "orderBy": "DESC"}' \
    --max-results 10
```

Atribut pengurutan yang tersedia adalah START_TIMEEND_TIME,STATUS,RISK_LEVEL,, danCONFIDENCE. Anda dapat mengurutkan dalam urutan ASC (naik) atau DESC (turun).

Contoh output:

```
{
    "Investigations": [
        {
            "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890",
            "Status": "COMPLETED",
            "TriggerPrompt": "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6
 in account 123456789012",
            "RiskLevel": "Critical",
            "Confidence": "High",
            "StartTime": 1705319400.0,
            "EndTime": 1705319700.0,
            "AccountId": "123456789012"
        },
        {
            "InvestigationId": "b2c3d4e5-6789-01bc-def0-ef2345678901",
            "Status": "COMPLETED",
            "TriggerPrompt": "Analyze findings in account with id 123456789012",
            "RiskLevel": "High",
            "Confidence": "High",
            "StartTime": 1705315800.0,
            "EndTime": 1705316100.0,
            "AccountId": "123456789012"
        },
        {
            "InvestigationId": "c3d4e5f6-7890-12cd-ef01-ef3456789012",
            "Status": "COMPLETED",
            "TriggerPrompt": "Analyze findings in my organization",
            "RiskLevel": "Medium",
            "Confidence": "Medium",
            "StartTime": 1705312200.0,
            "EndTime": 1705312500.0,
            "AccountId": "123456789012"
        }
    ]
}
```

Jika respons menyertakan `NextToken` nilai, berikan dalam permintaan berikutnya untuk mengambil halaman hasil berikutnya. Anda dapat mengambil hingga 50 hasil per halaman.

Aturan Deteksi Kustom di GuardDuty

Aturan Deteksi Kustom menyediakan pustaka aturan bawaan yang mendeteksi aktivitas yang tidak Anda harapkan terjadi di AWS lingkungan Anda. GuardDuty membangun dan memelihara aturan-aturan ini dan menjelaskan masing-masing menggunakan kosakata teknik ancaman mapan yang diambil dari katalog seperti MITRE ATT&CK® dan Katalog Teknik Ancaman. AWS Anda mengaktifkan setiap aturan untuk aktivitas yang ingin Anda deteksi, baik dalam mode dry run untuk mengukurnya terlebih dahulu atau mode langsung untuk menghasilkan temuan.

Tim keamanan sering tahu bahwa tindakan tertentu tidak boleh terjadi di akun tertentu. Tindakan seperti berbagi AMI, menghapus Log Aliran VPC, atau masuk tanpa MFA dapat dilakukan secara rutin di satu akun dan tanda kompromi di akun lain. Sebagian besar GuardDuty temuan mengidentifikasi aktivitas yang mencurigakan di lingkungan apa pun. Aturan Deteksi Kustom memungkinkan Anda mendeteksi aktivitas yang mencurigakan hanya di akun yang tidak Anda harapkan.

Aturan Deteksi Kustom menggunakan konsep-konsep berikut:

Aturan

Deteksi bawaan yang GuardDuty memiliki dan memelihara. Setiap aturan menargetkan satu teknik ancaman dan mendefinisikan kondisi yang menyebabkannya cocok.

Asosiasi

Tautan antara aturan dan akun. Asosiasi mencatat mode di mana aturan berjalan untuk akun itu. Aturan tanpa asosiasi tidak dievaluasi.

Modus

Perilaku aturan terkait saat cocok dengan aktivitas. Setiap aturan mendukung dua mode:

- Live — GuardDuty menghasilkan temuan saat aturan cocok dengan aktivitas. Mode langsung tidak kedaluwarsa.
- Dry run — GuardDuty mengevaluasi aturan dan memancarkan CloudWatch metrik Amazon tetapi tidak menghasilkan temuan. Gunakan dry run untuk mengukur volume sinyal sebelum Anda berkomitmen untuk deteksi langsung. GuardDuty memancarkan metrik ini hanya jika aturan cocok dengan suatu peristiwa, jadi aturan yang tidak pernah cocok tidak menghasilkan metrik dry run. Dry run secara otomatis kedaluwarsa setelah 14 hari.

Konfigurasi organisasi

Konfigurasi aturan bahwa akun GuardDuty administrator yang didelegasikan berlaku untuk akun anggota dalam organisasi. GuardDuty membuat asosiasi individu di setiap akun yang ditargetkan, termasuk akun yang bergabung nanti. Untuk informasi selengkapnya, lihat Mengelola Aturan Deteksi Kustom di lingkungan multi-akun.

Sinyal

Satu mengamati terjadinya aktivitas yang dideteksi oleh suatu aturan. GuardDutymenggabungkan sinyal terkait menjadi satu temuan. Untuk informasi selengkapnya, lihat Menemukan agregasi.

Topik

- Cara Kerja Aturan Deteksi Kustom
- Aturan Deteksi Kustom yang Tersedia
- Mengelola Aturan Deteksi Kustom
- Mengelola Aturan Deteksi Kustom di lingkungan multi-akun

Cara Kerja Aturan Deteksi Kustom

Mulailah dengan menelusuri aturan yang GuardDuty menawarkan untuk mengidentifikasi aturan yang mendeteksi aktivitas yang relevan dengan lingkungan Anda. Kemudian kaitkan setiap aturan dengan akun di mana aktivitas tidak terduga. Untuk informasi selengkapnya tentang mengaitkan aturan dengan akun, lihatMengelola Aturan Deteksi Kustom.

Sumber data dan sinyal

Setelah Anda mengaitkan aturan, GuardDuty memantau sumber data yang bergantung pada aturan dan mengevaluasi log masuk untuk peristiwa yang cocok. Aturan Deteksi Kustom mendukung acara AWS CloudTrail manajemen dan acara Runtime Monitoring. Ketika aktivitas yang diamati cocok dengan aturan, GuardDuty menghasilkan sinyal. Sinyal mewakili satu kejadian yang diamati dari aktivitas yang dideteksi aturan.

Setiap sumber data memiliki persyaratannya sendiri:

AWS CloudTrail acara manajemen

GuardDuty menganalisis peristiwa ini di setiap akun yang GuardDuty diaktifkan. Tidak diperlukan pengaturan tambahan.

Acara Runtime Monitoring

Aturan Runtime Monitoring mengevaluasi proses, file, dan aktivitas jaringan yang diamati agen GuardDuty keamanan pada sumber daya Anda. Aturan Runtime Monitoring hanya dapat mencocokkan aktivitas pada sumber daya yang memenuhi kedua persyaratan berikut:

- Runtime Monitoring diaktifkan untuk jenis sumber daya: Amazon EKS, Amazon EC2, atau Amazon ECS di Fargate. Untuk informasi selengkapnya, lihat GuardDuty Pemantauan Runtime.
- Agen GuardDuty keamanan berjalan pada sumber daya, pada atau di atas versi agen minimum aturan untuk platform itu.

Setiap aturan Runtime Monitoring menyatakan versi agen minimum yang diperlukan pada setiap platform di mana ia dapat berjalan. Untuk melihat persyaratan ini, hubungi GetCustomDetectionRuleoperasi.

Jika agen pada sumber daya lebih tua dari versi minimum aturan, aturan tidak cocok dengan aktivitas pada sumber daya tersebut. GuardDuty tidak melaporkan kesalahan dalam kasus ini, jadi perbarui agen tentang sumber daya tempat Anda mengaktifkan aturan Pemantauan Waktu Proses. Untuk informasi tentang versi agen, lihatGuardDuty versi rilis agen keamanan.

Modus

Setiap asosiasi berjalan dalam salah satu dari dua mode:

- Live — GuardDuty menghasilkan temuan ketika aturan cocok.
- Dry run — GuardDuty memancarkan CloudWatch metrik Amazon yang menghitung seberapa sering aturan cocok tetapi tidak menghasilkan temuan. Gunakan dry run untuk mengukur seberapa sering aturan cocok sebelum dapat membuat temuan atau memicu respons otomatis. Asosiasi lari kering kedaluwarsa 14 hari setelah pembuatan, asosiasi langsung tidak kedaluwarsa.

Untuk informasi selengkapnya, lihat Lari kering dan Hidup.

Menemukan agregasi

Setiap temuan mengikuti format`Tactic:Service/Technique`, misalnya, `Persistence:IAM/AccountManipulation` atau`Persistence:Runtime/SuspiciousCommand`. Bagaimana GuardDuty kelompok memberi sinyal ke dalam temuan tergantung pada sumber data yang menghasilkan sinyal, seperti yang dijelaskan dalam daftar berikut:

- AWS CloudTrail aturan — GuardDuty menggabungkan sinyal yang berbagi taktik, layanan, dan teknik yang sama menjadi satu temuan. Temuan tunggal dapat berisi beberapa sinyal ketika GuardDuty mengamati aktivitas yang sama berulang kali dari prinsip yang sama.
- Aturan Pemantauan Runtime — GuardDuty menggabungkan sinyal yang berbagi aturan, sumber daya, dan detail proses yang sama menjadi satu temuan. Setiap temuan mencakup satu sumber daya, seperti instance, tugas, atau wadah. Detail proses yang GuardDuty membandingkan tergantung pada jenis temuan. Misalnya, temuan modifikasi file juga membandingkan operasi file dan pengguna yang menjalankan proses. Pencocokan berulang memperbarui temuan yang ada alih-alih membuat yang baru. Temuan dari aturan yang berbeda tetap terpisah, bahkan ketika aturan menghasilkan jenis temuan yang sama untuk sumber daya dan proses yang sama.

Untuk informasi lebih lanjut tentang struktur dan bidang temuan, lihatAturan Deteksi Kustom menemukan detail.

Bidang acara yang disunting

aturan mengevaluasi bidang yang AWS CloudTrail merekam dalam suatu peristiwa. Redaksi terjadi di hulu. GuardDuty AWS Layanan dapat menyunting nilai bidang dalam peristiwa yang diterbitkan. Redaksi ini melindungi data yang berpotensi sensitif. Ketika bidang disunting, AWS CloudTrail mencatat bahwa bidang itu ada tetapi tidak mencatat nilainya.

Layanan yang menerbitkan acara memutuskan bidang mana yang disuntingnya. Layanan menyunting bidang ketika bidang itu dapat membawa informasi sensitif. Redaksi berlaku untuk bidang, bukan untuk nilai tertentu. Oleh karena itu, layanan menyunting bidang bahkan ketika nilai dalam permintaan tertentu tidak sensitif. Ini menyunting bidang tersebut untuk setiap permintaan, terlepas dari apakah Anda menggunakan Konsol Manajemen AWS, AWS CLI, atau AWS SDK.

GuardDuty tidak dapat mengevaluasi nilai yang tidak ada dalam acara tersebut. Jika logika deteksi aturan bergantung pada bidang yang disunting, aturannya tidak cocok. GuardDuty kemudian tidak menghasilkan sinyal dan tidak ada temuan, meskipun aktivitas terjadi. Aturan tidak terpengaruh jika hanya memeriksa bidang yang tidak disunting oleh layanan, seperti nama acara, AWS layanan, dan identitas panggilan.

Redaksi juga dapat membuat aturan cocok dengan satu permintaan tetapi tidak dengan permintaan lain yang memiliki efek yang sama. Ketika operasi API menerima lebih dari satu bidang untuk perubahan yang sama, satu bidang mungkin akan disunting dan yang lain mungkin tidak. Apakah aturan cocok kemudian tergantung pada bidang mana permintaan yang digunakan.

> **Note**
>
> Aturan Deteksi Kustom adalah kemampuan deteksi, bukan catatan audit lengkap. Untuk mengonfirmasi apakah panggilan API tertentu terjadi di akun Anda, tinjau peristiwa tersebut AWS CloudTrail. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat AWS CloudTrail acara.

Aturan Deteksi Kustom yang Tersedia

Aturan Deteksi Kustom memperluas deteksi ancaman yang GuardDuty disediakan. GuardDuty menawarkan pustaka aturan keikutsertaan yang dapat Anda pilih untuk diaktifkan berdasarkan risiko khusus untuk lingkungan Anda. Untuk mendapatkan daftar aturan yang tersedia saat ini, gunakan operasi ListCustomDetectionRulesAPI. Untuk jenis temuan yang dihasilkan setiap aturan, lihatJenis pencarian Aturan Deteksi Kustom.

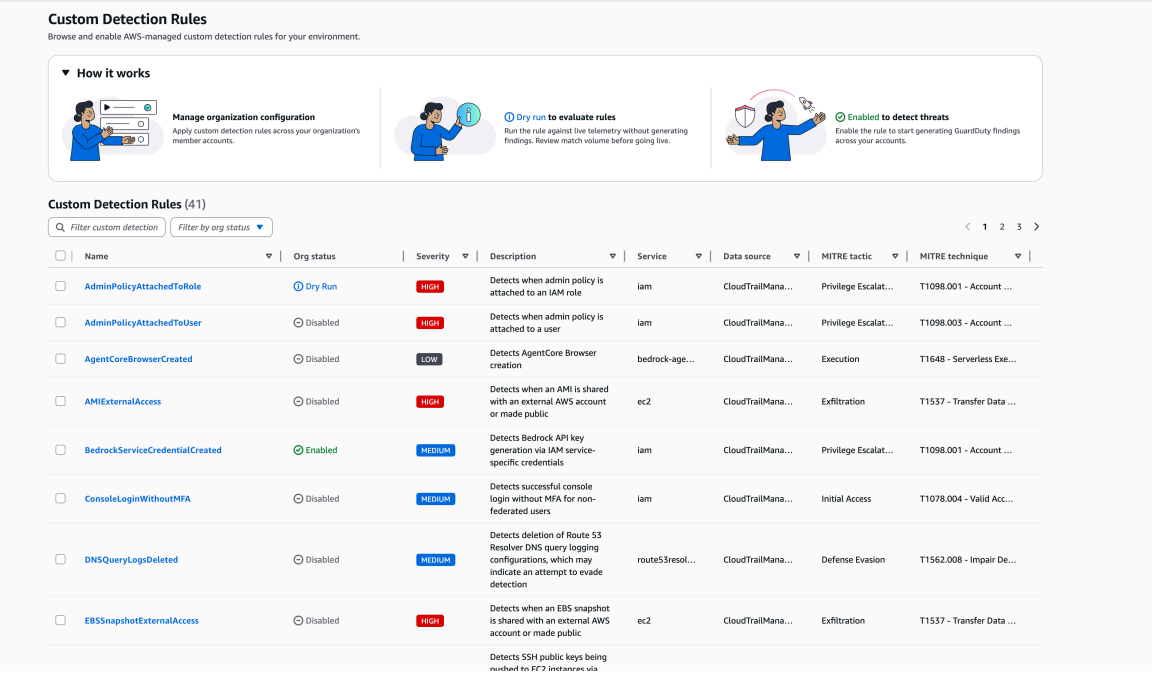
> **Note**
>
> Ketersediaan aturan individu tergantung pada ketersediaan AWS layanan dan fitur yang sesuai di setiap Wilayah. Misalnya, aturan yang menargetkan AWS Organizations atau Amazon Simple Email Service hanya tersedia di Wilayah tempat layanan tersebut beroperasi. Demikian pula, aturan yang menargetkan URL fungsi Lambda atau instance notebook SageMaker AI hanya tersedia di Wilayah di mana fitur tersebut didukung.

Melihat logika deteksi aturan

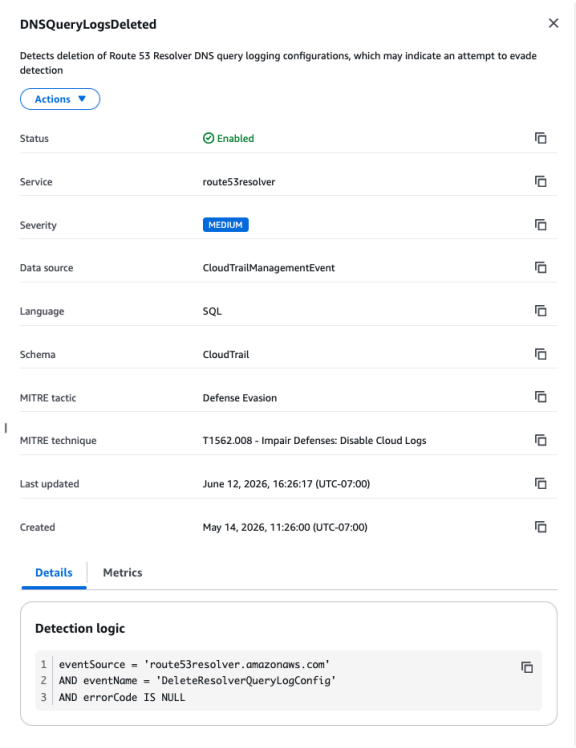
Setiap aturan mendefinisikan kondisi spesifik yang menentukan kapan kebakaran. Anda dapat memeriksa logika deteksi untuk aturan apa pun:

- Konsol — Di GuardDuty konsol, navigasikan ke Aturan Deteksi Kustom, dan pilih nama aturan. Panel split menampilkan logika deteksi aturan pada tab Detail.
- API — Panggil GetCustomDetectionRuleoperasi. Responsnya mencakup ekspresi aturan di `Definition.Expression` lapangan.

Gambar berikut menunjukkan katalog Aturan Deteksi Kustom.



Gambar berikut menunjukkan panel rincian aturan dengan logika deteksi.



Fungsi yang digunakan dalam logika deteksi

Aturan Deteksi Kustom menggunakan kondisi SQL. AWS CloudTrail aturan mengevaluasi bidang AWS CloudTrail peristiwa, dan beberapa menggunakan fungsi khusus untuk memeriksa struktur

JSON bersarang dalam bidang peristiwa seperti dan. `requestParameters` `responseElements` Aturan Runtime Monitoring mengevaluasi bidang peristiwa runtime, dan banyak yang menggunakan fungsi ekspresi reguler, terutama untuk mencocokkan baris perintah proses. Tabel berikut menjelaskan fungsi yang mungkin muncul dalam logika deteksi aturan.

Aturan yang memeriksa bidang bersarang bergantung pada bidang yang ada dalam acara tersebut. Untuk informasi selengkapnya tentang bidang yang AWS CloudTrail tidak direkam, lihatBidang acara yang disunting.

Fungsi	Pengembalian	Deskripsi
`get_json_object(json, path)`	String	Mengekstrak nilai dari dokumen JSON menggunakan jalur yang dipisahkan titik (misalnya,). `$.requestParameters.bucketName` Mengembalikan nilai sebagai string.
`json_collect_values(json, path, field)`	Array	Menavigasi ke array dalam dokumen JSON dan mengumpulkan bidang tertentu dari setiap elemen. Fungsi ini mengekstrak daftar nilai dari struktur berulang seperti pernyataan kebijakan IAM atau aturan grup keamanan.
`get_aws_principal(policy_json, effect)`	Array	Mem-parsing kebijakan sumber daya IAM, Amazon S3, atau Lambda dan mengembalikan prinsip akun dari pernyataan AWS yang cocok dengan efek yang ditentukan (Izinkan atau Tolak). Fungsi ini mendeteksi akses lintas akun dalam kebijakan sumber daya.
`policy_has_public_principal(policy_json, effect)`	Boolean	Mengembalikan nilai true ketika pernyataan dengan efek tertentu memberikan akses ke public principal (`"*"`). Fungsi ini mendeteksi kebijakan yang memungkinkan akses publik.
`RE2_FIND(input, pattern)`	Boolean	Mengembalikan nilai true ketika ekspresi reguler RE2 `pattern` cocok dengan bagian manapun dari. `input` Pertandingan ini peka huruf besar/

Fungsi	Pengembalian	Deskripsi
		kecil. Mengembalikan false `input` ketika null. Aturan Runtime Monitoring menggunakan fungsi ini terutama untuk mencocokkan baris perintah proses.
`IRE2_FIND(input, pattern)`	Boolean	Sama seperti`RE2_FIND`, tetapi pertandingan tidak peka huruf besar/kecil.

Agen GuardDuty keamanan mencatat argumen baris perintah proses yang dipisahkan oleh karakter null. Sebagian besar aturan Runtime Monitoring yang cocok dengan baris perintah pertama-tama mengganti pemisah ini dengan spasi, misalnya. `RE2_FIND(REPLACE(process.cmd_line, '\u0000', ' '), pattern)`

Logika deteksi SQL untuk aturan Runtime Monitoring adalah perkiraan bagaimana GuardDuty mendeteksi aktivitas, bukan logika yang tepat.

Mengelola Aturan Deteksi Kustom

GuardDuty menerapkan aturan ke akun melalui asosiasi. Asosiasi menautkan aturan ke akun Anda dan mencatat mode, live atau dry run, di mana aturan beroperasi.

Dalam organisasi, akun GuardDuty administrator yang didelegasikan menggunakan konfigurasi organisasi untuk mengelola aturan akun anggota secara terpusat. Konfigurasi organisasi mendukung menyertakan dan mengecualikan daftar untuk mengontrol akun mana yang berlaku aturan. Untuk informasi selengkapnya, lihat Mengelola Aturan Deteksi Kustom di lingkungan multi-akun.

Daftar aturan yang tersedia

Katalog aturan mencantumkan setiap aturan yang tersedia, dengan filter untuk nama, tingkat keparahan, sumber data, taktik MITRE ATT&CK®, teknik, dan AWS layanan.

Console

Untuk daftar aturan yang tersedia

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Aturan Deteksi Kustom.

3. Gunakan kontrol filter untuk mempersempit daftar berdasarkan properti (misalnya, tingkat keparahan atau taktik).

API/CLI

Jalankan ListCustomDetectionRulesoperasi. Anda dapat meneruskan filter untuk mempersempit hasil berdasarkan nama, tingkat keparahan, sumber data, taktik, teknik, atau layanan.

```
aws guardduty list-custom-detection-rules \
    --filters Name=severity,Values=HIGH
```

Melihat status aturan

Setiap aturan di akun Anda memiliki salah satu dari tiga status:

- Live — Aturan ini terkait dalam mode langsung dan menghasilkan temuan.
- Dry run — Aturan ini terkait dalam mode dry run dan hanya memancarkan CloudWatch metrik Amazon.
- Dinonaktifkan — Aturan tidak memiliki asosiasi dan tidak dievaluasi.

Console

Kolom Status pada halaman Aturan Deteksi Kustom menunjukkan status saat ini untuk setiap aturan. Anda dapat memfilter berdasarkan status menggunakan dropdown.

API/CLI

Jalankan ListCustomDetectionRuleAssociationsoperasi untuk melihat aturan mana yang terkait dengan akun Anda dan modenya saat ini.

```
aws guardduty list-custom-detection-rule-associations
```

Operasi massal

Operasi massal menerapkan perubahan mode yang sama ke lebih dari satu aturan, atau ke satu aturan di lebih dari satu akun.

Console

Pada halaman Aturan Deteksi Kustom, pilih beberapa aturan menggunakan kotak centang, lalu pilih Tindakan untuk mengaktifkan atau menonaktifkan semua aturan yang dipilih dalam satu tindakan.

API/CLI

Untuk menerapkan perubahan yang sama ke lebih dari satu aturan, panggil CreateCustomDetectionRuleAssociationsekali per aturan.

```
for RULE in rule-id-1 rule-id-2; do
    aws guardduty create-custom-detection-rule-association \
        --rule-id "$RULE" \
        --mode LIVE
done
```

Untuk menutupi setiap aturan dalam katalog dan bukan daftar bernama, ganti ID aturan dengan output dari ListCustomDetectionRules:`$(aws guardduty list-custom-detection-rules --query 'Rules[].RuleId' --output text)`.

Untuk menerapkan aturan tunggal ke banyak akun, gunakan konfigurasi organisasi alih-alih panggilan per akun. Konfigurasi organisasi menargetkan akun anggota dengan menyertakan dan mengecualikan daftar, dan GuardDuty membuat asosiasi individu. Untuk informasi selengkapnya, lihat Mengelola Aturan Deteksi Kustom di lingkungan multi-akun.

Lari kering

Dalam mode dry run, GuardDuty mengevaluasi peristiwa terhadap aturan tetapi tidak menghasilkan temuan. Sebagai gantinya, GuardDuty memancarkan CloudWatch metrik Amazon yang dapat Anda gunakan untuk mengevaluasi volume sinyal dan perilaku aturan sebelum mengaktifkan deteksi langsung. GuardDuty menerbitkan metrik ini hanya jika aturan cocok dengan suatu peristiwa; jika aturan tidak pernah cocok, itu tidak menghasilkan metrik dry run.

Gunakan mode dry run untuk memahami bagaimana aturan berperilaku di lingkungan Anda tanpa memicu respons otomatis atau menghasilkan temuan di konsol.

> **Note**
>
> Asosiasi dry run berakhir 14 hari setelah dibuat. Ketika kedaluwarsa, GuardDuty berhenti mengevaluasi aturan untuk akun itu dan aturan kembali dinonaktifkan. Untuk mengevaluasi aturan lagi, buat asosiasi dry run baru. Asosiasi langsung tidak kedaluwarsa.

Console

Untuk mengaktifkan aturan dalam mode dry run

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Aturan Deteksi Kustom.
3. Pilih satu atau beberapa aturan.
4. Pilih Actions, lalu pilih Enable (Dry Run).

API/CLI

Jalankan CreateCustomDetectionRuleAssociationoperasi dengan `mode` set ke`DRY_RUN`.

```
aws guardduty create-custom-detection-rule-association \
    --rule-id rule-id \
    --mode DRY_RUN
```

Hidup

Dalam mode langsung, GuardDuty menghasilkan temuan yang muncul di GuardDuty konsol. Temuan diekspor ke Amazon EventBridge dan, jika Anda mengonfigurasinya, ke bucket Amazon S3 yang Anda miliki. Temuan juga dikirim ke AWS layanan terintegrasi seperti AWS Security Hub. Gunakan mode langsung untuk deteksi ancaman aktif di lingkungan Anda.

Console

Untuk mengaktifkan aturan dalam mode langsung

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Aturan Deteksi Kustom.

3. Pilih satu atau beberapa aturan.
4. Pilih Tindakan, lalu pilih Aktifkan (Langsung).

Untuk mengalihkan aturan yang ada dari dry run ke live, pilih aturan, pilih Tindakan, lalu pilih Aktifkan (Langsung).

API/CLI

Untuk mengaktifkan aturan baru dalam mode langsung, jalankan CreateCustomDetectionRuleAssociationoperasi dengan `mode` set to`LIVE`.

```
aws guardduty create-custom-detection-rule-association \
    --rule-id rule-id \
    --mode LIVE
```

Untuk mengganti aturan yang ada dari dry run ke live, jalankan UpdateCustomDetectionRuleAssociationoperasi.

Menonaktifkan aturan

Menonaktifkan aturan akan menghapus asosiasi dan berhenti GuardDuty mengevaluasi peristiwa terhadap aturan tersebut untuk akun Anda.

Console

Untuk menonaktifkan Aturan Deteksi Kustom

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Aturan Deteksi Kustom.
3. Pilih satu atau beberapa aturan yang ingin Anda nonaktifkan.
4. Pilih Tindakan, lalu pilih Nonaktifkan.
5. Konfirmasikan tindakan saat diminta.

API/CLI

Jalankan DeleteCustomDetectionRuleAssociationoperasi.

```
aws guardduty delete-custom-detection-rule-association \
```

```
    --rule-id rule-id
```

Mengelola Aturan Deteksi Kustom di lingkungan multi-akun

Di organisasi, akun GuardDuty administrator yang didelegasikan mengelola Aturan Deteksi Kustom untuk akun anggota secara terpusat menggunakan konfigurasi organisasi. Administrator mendeklarasikan intent untuk setiap aturan, dan GuardDuty menerapkannya ke akun anggota secara otomatis, termasuk akun yang bergabung nanti.

> **Note**
>
> Multi-account pengelolaan Aturan Deteksi Kustom hanya didukung untuk akun yang dikelola melalui AWS Organizations. Invitation-based akun anggota tidak didukung untuk manajemen aturan terpusat.

Konfigurasi organisasi

Akun anggota tidak dapat mengaktifkan, menonaktifkan, atau mengubah Aturan Deteksi Kustom untuk dirinya sendiri. Jika Anda mencoba memanggil operasi asosiasi akun tunggal dari akun anggota, GuardDuty mengembalikan `AccessDeniedException` kesalahan. Administrator mengelola aturan atas nama anggota. Untuk informasi selengkapnya tentang akun administrator dan anggota yang didelegasikan, lihat Mengelola beberapa akun di GuardDuty.

Konfigurasi organisasi menautkan satu aturan ke satu set akun anggota. Ini merekam mode, live atau dry run, di mana aturan beroperasi untuk akun tersebut. GuardDuty kemudian membuat asosiasi individu untuk aturan di setiap akun anggota yang ditargetkan. Anda dapat mengonfigurasi aturan untuk semua anggota atau akun tertentu dengan menggunakan daftar sertakan dan kecualikan.

Console

Untuk mengonfigurasi Aturan Deteksi Kustom untuk organisasi

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Aturan Deteksi Kustom.
3. Pilih nama aturan untuk membuka detail aturan, lalu pilih tab Akun.
4. Pilih Konfigurasi di samping Konfigurasi Organisasi.

5. Pilih mode (Live atau Dry run) dan pilih akun mana yang akan disertakan atau dikecualikan.

API/CLI

Buat konfigurasi organisasi

Jalankan CreateCustomDetectionRuleOrgConfigurationuntuk membuat konfigurasi aturan untuk akun anggota.

Memperbarui konfigurasi organisasi

Jalankan UpdateCustomDetectionRuleOrgConfigurationuntuk mengubah mode atau cakupan akun.

Menghapus konfigurasi organisasi

Jalankan DeleteCustomDetectionRuleOrgConfigurationuntuk menghapus konfigurasi organisasi. Karena aturan dapat menahan satu konfigurasi per mode, `mode` pilih mana yang akan dihapus; yang lain dibiarkan di tempat.

> **Note**
>
> Menghapus konfigurasi organisasi tidak akan menghapus asosiasi akun anggota yang ada. Aturan tetap diaktifkan di akun anggota yang GuardDuty telah menerapkannya.

> **Note**
>
> Konfigurasi organisasi dry run akan kedaluwarsa 14 hari setelah Anda membuatnya. Asosiasi akun anggota yang GuardDuty dibuat dari konfigurasi itu kedaluwarsa dengannya, bukan 14 hari setelah setiap asosiasi dibuat.

Menjalankan kedua mode untuk aturan yang sama

Aturan memegang paling banyak satu konfigurasi organisasi per mode, sehingga aturan dapat berjalan dalam mode langsung dan mode dry run pada saat yang sama hanya dalam kondisi berikut: kedua konfigurasi harus memberi nama akun target mereka dengan daftar sertakan eksplisit.

Konfigurasi yang mengklaim seluruh organisasi adalah satu kesempatan untuk aturannya. Konfigurasi mengklaim seluruh organisasi ketika tidak menamai akun sama sekali, atau ketika menamai akun untuk dikecualikan. Tidak ada konfigurasi untuk mode lain yang dapat hidup berdampingan dengannya, dan mencoba membuatnya kembali. `ConflictException` Untuk memindahkan konfigurasi seluruh organisasi ke mode yang berbeda, perbarui konfigurasi yang ada alih-alih membuat yang kedua.

Contoh: Menerapkan aturan dalam mode dry run ke semua akun anggota

Perintah AWS CLI berikut membuat konfigurasi organisasi yang menargetkan setiap akun anggota, termasuk akun yang bergabung nanti. Menghilangkan keduanya `--include-account-ids` dan `--exclude-account-ids` menargetkan seluruh organisasi.

```
aws guardduty create-custom-detection-rule-org-configuration \
    --rule-id "EXAMPLE_RULE_ID" \
    --mode DRY_RUN
```

Untuk memindahkan aturan ke deteksi langsung, perbarui konfigurasi yang ada dengan UpdateCustomDetectionRuleOrgConfiguration.

Menerapkan setiap aturan di seluruh organisasi

Konsol mengkonfigurasi satu aturan pada satu waktu. Untuk menerapkan mode yang sama ke setiap aturan yang tersedia di seluruh organisasi, ulangi katalog aturan dengan AWS CLI. Menghilangkan keduanya `--include-account-ids` dan `--exclude-account-ids` menargetkan setiap akun anggota, termasuk akun yang bergabung nanti.

```
for RULE in $(aws guardduty list-custom-detection-rules \
    --query 'Rules[].RuleId' --output text); do
    aws guardduty create-custom-detection-rule-org-configuration \
        --rule-id "$RULE" \
        --mode DRY_RUN
done
```

Loop ini digunakan `--mode DRY_RUN` sehingga Anda dapat mengukur volume sinyal sebelum aturan apa pun menghasilkan temuan. Karena loop tidak menamai akun, setiap konfigurasi mengklaim seluruh organisasi dan merupakan satu kesempatan untuk aturannya. Saat Anda siap, pindahkan setiap aturan ke deteksi langsung dengan memperbarui konfigurasi yang ada

UpdateCustomDetectionRuleOrgConfiguration. Menjalankan loop lagi dengan `--mode LIVE` pengembalian`ConflictException`, karena konfigurasi dry run seluruh organisasi sudah ada.

Mengelola banyak akun di Amazon GuardDuty

Ketika AWS lingkungan Anda memiliki beberapa akun, Anda dapat mengelolanya dengan menunjuk satu Akun AWS sebagai akun administrator. Anda kemudian dapat mengaitkan beberapa Akun AWS dengan akun administrator ini sebagai akun anggotanya. Dengan konfigurasi ini, akun GuardDuty administrator yang ditunjuk dapat menilai dan memantau keamanan keseluruhan organisasi Anda. Akun administrator juga dapat melakukan tugas manajemen akun, seperti meninjau semua temuan yang dihasilkan dan mengonfigurasi rencana perlindungan di dalamnya. GuardDuty

Dalam GuardDuty, organisasi terdiri dari akun GuardDuty administrator yang didelegasikan dan satu atau lebih akun anggota terkait. Anda dapat mengaitkan akun dengan dua cara — dengan mengintegrasikan dengan AWS Organizations, atau dengan menggunakan metode lama mengirim dan menerima undangan keanggotaan di konsol. GuardDuty GuardDuty merekomendasikan agar Anda berintegrasi dengan AWS Organizations.

> **Note**
>
> Tombol Edit di bagian aktifkan otomatis pada halaman Akun mengarahkan Anda ke Mengkonfigurasi rencana perlindungan halaman alih-alih membuka modal konfigurasi lama.

AWS Organizations adalah layanan manajemen akun global yang memungkinkan AWS administrator untuk mengkonsolidasikan dan mengelola beberapa secara terpusat. Akun AWS Ini menyediakan manajemen akun dan fitur penagihan konsolidasi yang dirancang untuk mendukung kebutuhan anggaran, keamanan, dan kepatuhan. Ini ditawarkan tanpa biaya tambahan dan terintegrasi dengan beberapa Layanan AWS, termasuk Macie, AWS Security Hub CSPM, dan Amazon. GuardDuty Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Organizations.

Daftar Isi

- Memahami hubungan antara akun GuardDuty administrator dan akun anggota
- Mengelola GuardDuty akun dengan AWS Organizations
- Mengelola akun menggunakan kebijakan organisasi
- Mengelola GuardDuty akun dengan undangan
- GuardDuty pertimbangan untuk mengekspor detail akun anggota dalam format CSV

Memahami hubungan antara akun GuardDuty administrator dan akun anggota

Saat Anda menggunakan GuardDuty di lingkungan beberapa akun, akun administrator dapat mengelola aspek-aspek tertentu GuardDuty atas nama akun anggota. Akun administrator dapat melakukan fungsi utama berikut:

- Menambah dan menghapus akun anggota terkait — Proses di mana akun administrator dapat melakukan ini berbeda berdasarkan cara Anda mengelola akun — melalui AWS Organizations atau dengan metode GuardDuty undangan.

  GuardDuty merekomendasikan mengelola akun anggota Anda melalui AWS Organizations.
- Akun GuardDuty administrator yang didelegasikan mengaktifkan GuardDuty akun manajemen — Jika akun AWS Organizations manajemen pernah dinonaktifkan GuardDuty, akun GuardDuty administrator yang didelegasikan dapat diaktifkan GuardDuty di akun manajemen. Namun, diperlukan bahwa akun manajemen harus belum secara eksplisit menghapus. Service-linked izin peran untuk GuardDuty
- Konfigurasi status akun anggota — Akun administrator dapat mengaktifkan atau menonaktifkan status rencana GuardDuty perlindungan, dan mengaktifkan, menangguhkan, atau menonaktifkan status GuardDuty atas nama akun anggota terkait.

  Akun GuardDuty administrator yang didelegasikan yang dikelola dengan AWS Organizations dapat secara otomatis mengaktifkan GuardDuty ketika Akun AWS ditambahkan sebagai anggota.
- Sesuaikan kapan harus menghasilkan temuan — Akun administrator dapat menyesuaikan temuan dalam GuardDuty jaringan dengan membuat dan mengelola aturan penindasan, daftar IP tepercaya, dan daftar ancaman. Dalam lingkungan multi-akun, dukungan untuk mengonfigurasi fitur ini hanya tersedia untuk akun administrator yang GuardDuty didelegasikan. Akun anggota tidak dapat memperbarui konfigurasi ini.

Tabel berikut merinci hubungan antara akun GuardDuty administrator dan akun anggota.

Kunci untuk tabel

- Self — Akun dapat melakukan tindakan yang terdaftar hanya untuk akun mereka sendiri.
- Apa saja — Akun dapat melakukan tindakan yang tercantum untuk akun terkait apa pun.

- Semua — Akun dapat melakukan tindakan yang tercantum dan berlaku untuk semua akun terkait. Biasanya, akun yang mengambil tindakan ini adalah akun GuardDuty administrator yang ditunjuk
- Sel dengan tanda hubung (—) — Sel tabel dengan tanda hubung (—) menunjukkan bahwa akun tidak dapat melakukan tindakan yang tercantum.

Tindakan	Melalui AWS Organizations		Dengan undangan	
	Akun GuardDuty administrator yang didelegasikan	Akun anggota terkait	GuardDuty akun administrator	Akun anggota terkait
Aktifkan GuardDuty	Setiap	–	Mandiri	Mandiri
Aktifkan GuardDuty secara otomatis untuk seluruh organisasi (`ALL`,`NEW`,`NONE`)	Semua	–	–	–
Lihat semua akun anggota Organizations terlepas dari GuardDuty statusnya	Setiap	–	–	–
Membuat temuan sampel	Mandiri	Mandiri	Mandiri	Mandiri
Lihat semua GuardDuty temuan	Setiap	Mandiri	Setiap	Mandiri

GuardDuty Temuan arsip	Setiap	–	Setiap	–
Menerapkan aturan penekanan	Semua	–	Semua	–
Buat daftar IP tepercaya atau daftar ancaman	Semua	–	Semua	–
Perbarui daftar IP tepercaya atau daftar ancaman	Semua	–	Semua	–
Hapus daftar IP tepercaya atau daftar ancaman	Semua	–	Semua	–
Atur frekuensi EventBridge notifikasi	Semua	–	Semua	–
Mengatur lokasi Amazon S3 untuk mengekspor temuan	Semua	Mandiri	Mandiri	Mandiri

Aktifkan satu atau lebih rencana perlindungan opsional untuk seluruh organisasi (`ALL`,`NEW`,`NONE`) Ini tidak termasuk Perlindungan Malware untuk S3.	Semua	–	–	–
Aktifkan paket GuardDuty perlindungan apa pun untuk akun individu Ini tidak termasuk Perlindungan Malware untuk EC2 dan Perlindungan Malware untuk S3.	Setiap	–	Setiap	–
Perlindungan Malware untuk EC2	Setiap	–	Mandiri	–

Perlindungan Malware untuk EC2 - pemindaian On-demand malware	Setiap	Mandiri	Mandiri	Mandiri
Perlindungan Malware untuk S3	–	Mandiri	–	Mandiri
Pisahkan akun anggota	Apa saja [+]	–	Setiap	–
Pisahkan dari akun administrator	–	–	–	Mandiri
Menghapus akun anggota yang tidak terkait	Setiap	–	Setiap	–
Menangguhkan GuardDuty	* Apa saja*	–	* Apa saja*	–
Nonaktifkan GuardDuty	* Apa saja*	–	* Apa saja*	Mandiri

[+] Menunjukkan bahwa akun GuardDuty administrator yang didelegasikan dapat mengambil tindakan ini hanya jika mereka belum menyiapkan preferensi aktifkan otomatis ke ALL anggota organisasi.

[*] Menunjukkan bahwa akun GuardDuty administrator yang didelegasikan tidak dapat menonaktifkan GuardDuty di akun anggota secara langsung. Akun GuardDuty administrator yang didelegasikan harus terlebih dahulu memisahkan akun anggota, dan kemudian menghapusnya. Setelah ini, setiap akun anggota dapat menonaktifkan GuardDuty di akun mereka sendiri. Untuk informasi selengkapnya tentang melakukan tugas-tugas ini di organisasi Anda, lihatTerus mengelola akun anggota Anda dalam GuardDuty.

Memahami status hubungan anggota

GuardDuty Operasi API seperti ListMembersdan GetMembersmengembalikan `relationshipStatus` bidang untuk setiap akun anggota. Bidang ini menunjukkan keadaan hubungan saat ini antara akun administrator dan akun anggota. Periksa nilai ini ketika Anda ingin mengonfirmasi bahwa GuardDuty secara aktif memantau akun anggota. Ini juga membantu Anda memecahkan masalah mengapa akun anggota tidak menyelesaikan orientasi atau tidak lagi dipantau. Daftar berikut menjelaskan nilai yang mungkin.

`Created`

Akun administrator telah menambahkan akun ini sebagai anggota (misalnya, dengan meneleponCreateMembers), tetapi hubungan anggota belum aktif.

`Invited`

Akun administrator telah mengirim undangan ke akun anggota ini, dan undangan menunggu untuk diterima.

`Enabled`

Akun anggota ini dikaitkan dengan akun administrator, dan GuardDuty secara aktif memantau akun anggota.

`Disabled`

Akun anggota ini dikaitkan dengan akun administrator, tetapi GuardDuty tidak secara aktif memantau akun anggota.

`Removed`

Akun anggota ini tidak lagi terkait dengan akun administrator. Status ini biasanya menunjukkan bahwa akun administrator menghapus asosiasi.

`Resigned`

Akun anggota ini tidak lagi terkait dengan akun administrator. Status ini biasanya menunjukkan bahwa akun anggota dihapus sendiri dari asosiasi.

`Deleted`

Akun anggota ini tidak ada lagi GuardDuty.

`EmailVerificationInProgress`

Undangan akun anggota ini sedang menunggu verifikasi alamat email.

`EmailVerificationFailed`

Undangan akun anggota ini tidak lolos verifikasi alamat email.

`RegionDisabled`

Akun anggota ini tidak dapat dipantau karena GuardDuty tidak diaktifkan atau tidak tersedia saat ini Wilayah AWS.

`AccountSuspended`

Anggota Akun AWS ini dalam keadaan ditangguhkan.

`CannotCreateDetectorInOrganizationMasterAccount`

GuardDuty tidak dapat membuat detektor di akun AWS Organizations manajemen, biasanya karena izin peran terkait layanan yang diperlukan tidak ada.

Mengelola GuardDuty akun dengan AWS Organizations

Dalam suatu AWS organisasi, akun manajemen dapat menunjuk akun apa pun dalam organisasi ini sebagai akun GuardDuty administrator yang didelegasikan. Untuk akun administrator ini, GuardDuty akan diaktifkan secara otomatis hanya di saat ini Wilayah AWS. Secara default, akun administrator dapat mengaktifkan dan mengelola GuardDuty semua akun anggota di organisasi dalam Wilayah tersebut. Akun administrator dapat melihat dan menambahkan anggota ke AWS organisasi ini.

Bagian berikut akan memandu Anda melalui berbagai tugas yang dapat Anda lakukan sebagai akun GuardDuty administrator yang didelegasikan.

Daftar Isi

- Pertimbangan dan rekomendasi untuk digunakan dengan GuardDuty AWS Organizations
- Izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty
- Menunjuk akun administrator yang didelegasikan GuardDuty
- Menyetel preferensi aktifkan otomatis organisasi
- Menambahkan anggota ke organisasi
- (Opsional) Aktifkan paket perlindungan untuk akun anggota yang ada
- Terus mengelola akun anggota Anda dalam GuardDuty
- Penangguhan GuardDuty untuk akun anggota

- Memutuskan (menghapus) akun anggota dari akun administrator
- Menghapus akun anggota dari organisasi GuardDuty
- Mengubah akun GuardDuty administrator yang didelegasikan

Pertimbangan dan rekomendasi untuk digunakan dengan GuardDuty AWS Organizations

Pertimbangan dan rekomendasi berikut dapat membantu Anda memahami cara operasi akun GuardDuty administrator yang didelegasikan: GuardDuty

Akun GuardDuty administrator yang didelegasikan dapat mengelola maksimal 50.000 anggota.

> Ada batas 50.000 akun anggota per akun GuardDuty administrator yang didelegasikan. Ini termasuk akun anggota yang ditambahkan melalui AWS Organizations atau mereka yang menerima undangan akun GuardDuty administrator untuk bergabung dengan organisasi mereka. Namun, mungkin ada lebih dari 50.000 akun di AWS organisasi Anda.
>
> Jika Anda melebihi batas 50.000 akun anggota, Anda akan menerima pemberitahuan dari CloudWatch, Dasbor Health, dan email ke akun GuardDuty administrator yang didelegasikan yang ditunjuk.

Akun GuardDuty administrator yang didelegasikan adalah Regional.

> Tidak seperti AWS Organizations, GuardDuty adalah layanan Regional. Akun GuardDuty administrator yang didelegasikan dan akun anggotanya harus ditambahkan AWS Organizations di setiap Wilayah yang diinginkan tempat Anda telah GuardDuty mengaktifkan. Jika akun manajemen organisasi menunjuk akun GuardDuty administrator yang didelegasikan hanya di AS Timur (Virginia N.), maka akun GuardDuty administrator yang didelegasikan hanya akan mengelola akun anggota yang ditambahkan ke organisasi di Wilayah tersebut. Untuk informasi selengkapnya tentang paritas fitur di Wilayah GuardDuty yang tersedia, lihatWilayah dan titik akhir.

Kasus khusus untuk Wilayah keikutsertaan

- Ketika akun GuardDuty administrator yang didelegasikan memilih keluar dari Wilayah keikutsertaan, meskipun organisasi Anda memiliki konfigurasi GuardDuty aktifkan otomatis yang disetel ke akun anggota baru saja (`NEW`) atau semua akun anggota (`ALL`), GuardDuty tidak dapat diaktifkan untuk akun anggota mana pun di organisasi yang saat ini telah dinonaktifkan. GuardDuty Untuk informasi tentang konfigurasi akun anggota Anda, buka Akun di panel navigasi GuardDuty konsol atau gunakan ListMembersAPI.

- Saat bekerja dengan konfigurasi GuardDuty aktifkan otomatis yang disetel ke`NEW`, pastikan urutan berikut terpenuhi:

  1. Akun anggota ikut serta ke Wilayah keikutsertaan.
  2. Tambahkan akun anggota ke organisasi Anda di AWS Organizations.

  Jika Anda mengubah urutan langkah-langkah ini, pengaturan GuardDuty aktifkan otomatis dengan tidak **`NEW`** akan berfungsi di Wilayah keikutsertaan tertentu karena akun anggota tidak lagi baru bagi organisasi. GuardDuty menyediakan dua solusi alternatif:

  - Setel konfigurasi GuardDuty aktifkan otomatis ke`ALL`, yang mencakup akun anggota baru dan yang sudah ada. Dalam hal ini, urutan langkah-langkah ini tidak relevan.
  - Jika akun anggota sudah menjadi bagian dari organisasi Anda, kelola GuardDuty konfigurasi untuk akun ini secara individual di Wilayah keikutsertaan tertentu dengan menggunakan GuardDuty konsol atau API.

Diperlukan agar AWS organisasi memiliki akun GuardDuty administrator yang didelegasikan yang sama di semua akun. Wilayah AWS

Anda harus menetapkan satu akun anggota sebagai akun GuardDuty administrator yang didelegasikan di semua Wilayah AWS tempat GuardDuty diaktifkan. Misalnya, jika Anda menunjuk akun *`111122223333`* anggota*`Europe (Ireland)`*, Anda tidak dapat menunjuk akun *`555555555555`* anggota lain. *`Canada (Central)`* Anda harus menggunakan akun yang sama dengan akun GuardDuty administrator yang didelegasikan di semua Wilayah lainnya.

Anda dapat menunjuk akun GuardDuty administrator yang didelegasikan baru kapan saja. Untuk informasi selengkapnya tentang menghapus akun GuardDuty administrator terdelegasi yang ada, lihatMengubah akun GuardDuty administrator yang didelegasikan.

Tidak disarankan untuk menetapkan akun manajemen organisasi Anda sebagai akun GuardDuty administrator yang didelegasikan.

Akun manajemen organisasi Anda dapat berupa akun GuardDuty administrator yang didelegasikan. Namun, praktik terbaik AWS keamanan mengikuti prinsip hak istimewa paling sedikit dan tidak merekomendasikan konfigurasi ini.

Mengubah akun GuardDuty administrator yang didelegasikan tidak menonaktifkan GuardDuty akun anggota.

Jika Anda menghapus akun GuardDuty administrator yang didelegasikan, GuardDuty hapus semua akun anggota yang terkait dengan akun GuardDuty administrator yang didelegasikan ini. GuardDuty masih tetap diaktifkan untuk semua akun anggota ini.

Izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty

Untuk mulai menggunakan Amazon GuardDuty dengan AWS Organizations, akun AWS Organizations manajemen untuk organisasi menetapkan akun sebagai akun GuardDuty administrator yang didelegasikan. Ini memungkinkan GuardDuty sebagai layanan tepercaya di AWS Organizations. Ini juga memungkinkan GuardDuty akun GuardDuty administrator yang didelegasikan dan juga memungkinkan akun administrator yang didelegasikan untuk mengaktifkan dan mengelola GuardDuty akun lain di organisasi di Wilayah saat ini. Untuk informasi tentang cara izin ini diberikan, lihat Menggunakan AWS Organizations dengan AWS layanan lain.

Sebagai akun AWS Organizations manajemen, sebelum Anda menetapkan akun GuardDuty administrator yang didelegasikan untuk organisasi Anda, verifikasi bahwa Anda dapat melakukan GuardDuty tindakan berikut: `guardduty:EnableOrganizationAdminAccount` Tindakan ini memungkinkan Anda untuk menunjuk akun GuardDuty administrator yang didelegasikan untuk organisasi Anda dengan menggunakan. GuardDuty Anda juga harus memastikan bahwa Anda diizinkan untuk melakukan AWS Organizations tindakan yang membantu Anda mengambil informasi tentang organisasi Anda.

Untuk memberikan izin ini, sertakan pernyataan berikut dalam kebijakan AWS Identity and Access Management (IAM) untuk akun Anda:

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListRoots"
    ],
    "Resource": "*"
}
```

Jika Anda ingin menetapkan akun AWS Organizations manajemen Anda sebagai akun GuardDuty administrator yang didelegasikan, akun Anda juga akan memerlukan tindakan IAM:. `CreateServiceLinkedRole` Tindakan ini memungkinkan Anda untuk menginisialisasi GuardDuty untuk akun manajemen. Namun, tinjau Pertimbangan dan rekomendasi untuk digunakan dengan GuardDuty AWS Organizations sebelum Anda melanjutkan untuk menambahkan izin.

Untuk melanjutkan penunjukan akun manajemen sebagai akun GuardDuty administrator yang didelegasikan, tambahkan pernyataan berikut ke kebijakan IAM dan ganti *111122223333* dengan Akun AWS ID akun manajemen organisasi Anda:

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
 }
}
```

Menunjuk akun administrator yang didelegasikan GuardDuty

Bagian ini menyediakan langkah-langkah untuk menunjuk administrator yang didelegasikan dalam organisasi. GuardDuty

Sebagai akun manajemen AWS organisasi, pastikan Anda membaca Pertimbangan dan rekomendasi tentang cara akun GuardDuty administrator yang didelegasikan beroperasi. Sebelum melanjutkan, pastikan Anda memilikinyaIzin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty.

Pilih metode akses yang disukai untuk menunjuk akun GuardDuty administrator yang didelegasikan untuk organisasi Anda. Hanya akun manajemen yang dapat melakukan langkah ini.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

Untuk masuk, gunakan kredensyal akun manajemen untuk organisasi Anda AWS Organizations .

2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menunjuk akun administrator yang didelegasikan GuardDuty untuk organisasi Anda.
3. Lakukan salah satu hal berikut, tergantung pada apakah GuardDuty diaktifkan untuk akun manajemen Anda di Wilayah saat ini:

   - Jika tidak GuardDuty diaktifkan, pilih Amazon GuardDuty - semua fitur dan pilih Mulai. Tindakan ini akan membawa Anda ke GuardDuty halaman Selamat Datang di.
   - Jika GuardDuty diaktifkan, pilih Pengaturan di panel navigasi.
4. Di bawah Administrator yang didelegasikan, masukkan Akun AWS ID 12 digit akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator yang didelegasikan untuk organisasi.
5. Pilih Delegasikan.
6. (Disarankan) Ulangi langkah-langkah sebelumnya untuk menunjuk akun GuardDuty administrator yang didelegasikan di setiap Wilayah AWS tempat yang telah Anda aktifkan. GuardDuty

API/CLI

1. Jalankan enableOrganizationAdminAccountmenggunakan kredensi Akun AWS akun manajemen organisasi.

   - Atau, Anda dapat menggunakannya AWS Command Line Interface untuk melakukan ini. AWS CLI Perintah berikut menunjuk akun GuardDuty administrator yang didelegasikan untuk Wilayah Anda saat ini saja. Jalankan AWS CLI perintah berikut dan pastikan untuk mengganti *111111111111* dengan Akun AWS ID akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator yang didelegasikan:

     ```
     aws guardduty enable-organization-admin-account --admin-account-
     id 111111111111
     ```

     Untuk menunjuk akun GuardDuty administrator yang didelegasikan untuk Wilayah lain, tentukan Wilayah dalam perintah. AWS CLI Contoh berikut menunjukkan cara mengaktifkan akun GuardDuty administrator yang didelegasikan di AS Barat (Oregon).

Pastikan untuk mengganti *us-west-2* dengan Wilayah yang ingin Anda tetapkan akun GuardDuty administrator yang didelegasikan.

```
aws guardduty enable-organization-admin-account --admin-account-
id 111111111111 --region us-west-2
```

Untuk informasi tentang Wilayah AWS tempat GuardDuty tersedia, lihatWilayah dan titik akhir.

Jika GuardDuty dinonaktifkan untuk akun GuardDuty administrator yang didelegasikan, akun tersebut tidak akan dapat mengambil tindakan apa pun. Jika belum dilakukan, pastikan GuardDuty untuk mengaktifkan akun GuardDuty administrator delegasi yang baru ditunjuk.

2. (Disarankan) ulangi langkah-langkah sebelumnya untuk menunjuk akun GuardDuty administrator yang didelegasikan di setiap Wilayah AWS tempat yang telah Anda aktifkan. GuardDuty

Menyetel preferensi aktifkan otomatis organisasi

Fitur mengaktifkan otomatis organisasi di GuardDuty membantu Anda mengatur status paket perlindungan yang sama GuardDuty untuk akun `ALL` yang ada atau `NEW` anggota di organisasi Anda, dalam satu langkah. Demikian pula, Anda juga dapat menentukan kapan Anda tidak ingin mengambil tindakan apa pun pada akun anggota, dengan memilih`NONE`. Langkah-langkah berikut menjelaskan pengaturan ini dan juga menunjukkan kapan Anda ingin menggunakan pengaturan tertentu.

> **Note**
>
> Anda dapat mengatur preferensi aktifkan otomatis untuk semua paket perlindungan kecualiPerlindungan Malware untuk S3.

Pilih metode akses yang disukai untuk memperbarui preferensi aktifkan otomatis untuk organisasi.

Console

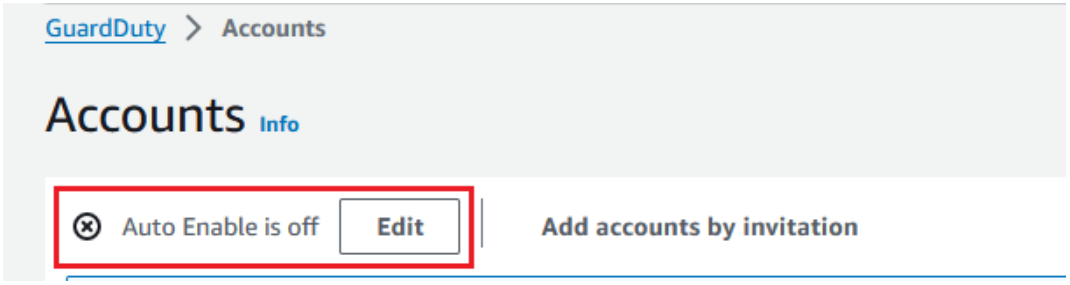
1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Untuk masuk, gunakan GuardDuty kredensil akun administrator.

2. Di panel navigasi, pilih Akun.

Halaman Akun menyediakan opsi konfigurasi ke akun GuardDuty administrator Auto-enable GuardDuty dan paket perlindungan opsional atas nama akun anggota milik organisasi.

3. Untuk memperbarui pengaturan aktifkan otomatis yang ada, pilih Edit.



Dukungan ini tersedia untuk dikonfigurasi GuardDuty dan semua paket perlindungan opsional yang didukung di Anda Wilayah AWS. Anda dapat memilih salah satu opsi konfigurasi berikut untuk GuardDuty atas nama akun anggota Anda:

- Aktifkan untuk semua akun (**`ALL`**) — Pilih untuk mengaktifkan opsi yang sesuai untuk semua akun dalam organisasi. Ini termasuk akun baru yang bergabung dengan organisasi dan akun yang mungkin telah ditangguhkan atau dihapus dari organisasi. Ini juga termasuk akun GuardDuty administrator yang didelegasikan.

  > **Note**
  >
  > Diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota.

- Auto-enable untuk akun baru (**`NEW`**) — Pilih untuk mengaktifkan GuardDuty atau paket perlindungan opsional hanya untuk akun anggota baru secara otomatis ketika mereka bergabung dengan organisasi Anda.
- Jangan aktifkan (**`NONE`**) — Pilih untuk mencegah mengaktifkan opsi yang sesuai untuk akun baru di organisasi Anda. Dalam hal ini, akun GuardDuty administrator akan mengelola setiap akun secara individual.

  Saat Anda memperbarui pengaturan aktifkan otomatis dari `ALL` atau `NEW` ke`NONE`, tindakan ini tidak menonaktifkan opsi terkait untuk akun Anda yang ada. Konfigurasi ini akan berlaku untuk akun baru yang bergabung dengan organisasi. Setelah Anda memperbarui pengaturan aktifkan otomatis, tidak ada akun baru yang akan memiliki opsi yang sesuai sebagaimana diaktifkan.

> **Note**
>
> Ketika akun GuardDuty administrator yang didelegasikan memilih keluar dari Wilayah keikutsertaan, meskipun organisasi Anda memiliki konfigurasi GuardDuty aktifkan otomatis yang disetel ke akun anggota baru saja (`NEW`) atau semua akun anggota (`ALL`), GuardDuty tidak dapat diaktifkan untuk akun anggota mana pun di organisasi yang saat ini telah dinonaktifkan. GuardDuty Untuk informasi tentang konfigurasi akun anggota Anda, buka Akun di panel navigasi GuardDuty konsol atau gunakan ListMembersAPI.

4. Pilih Simpan perubahan.
5. (Opsional) jika Anda ingin menggunakan preferensi yang sama di setiap Wilayah, perbarui preferensi Anda di setiap Wilayah yang didukung secara terpisah.

   Beberapa paket perlindungan opsional mungkin tidak tersedia di semua Wilayah AWS tempat yang GuardDuty tersedia. Untuk informasi selengkapnya, lihat Wilayah dan titik akhir.

API/CLI

1. Jalankan UpdateOrganizationConfigurationdengan menggunakan kredensil akun GuardDuty administrator yang didelegasikan, untuk secara otomatis mengonfigurasi GuardDuty dan rencana perlindungan opsional di Wilayah tersebut untuk organisasi Anda. Untuk informasi tentang berbagai konfigurasi auto-enable, lihat auto. EnableOrganizationMembers

   Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

   Untuk mengatur preferensi aktifkan otomatis untuk salah satu paket perlindungan opsional yang didukung di Wilayah Anda, ikuti langkah-langkah yang disediakan di bagian dokumentasi terkait dari setiap paket perlindungan.
2. Anda dapat memvalidasi preferensi untuk organisasi Anda di Wilayah saat ini. Jalankan describeOrganizationConfiguration. Pastikan untuk menentukan ID detektor dari akun GuardDuty administrator yang didelegasikan.

> **Note**
>
> Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota.

3. Atau, jalankan AWS CLI perintah berikut untuk mengatur preferensi agar mengaktifkan atau menonaktifkan secara otomatis GuardDuty di Region untuk akun baru (`NEW`) yang bergabung dengan organisasi, semua akun (`ALL`), atau tidak ada akun (`NONE`) di organisasi. Untuk informasi selengkapnya, lihat auto EnableOrganizationMembers. Berdasarkan preferensi Anda, Anda mungkin perlu mengganti `NEW` dengan `ALL` atau`NONE`. Jika Anda mengonfigurasi paket perlindungan dengan`ALL`, paket perlindungan juga akan diaktifkan untuk akun GuardDuty administrator yang didelegasikan. Pastikan untuk menentukan ID detektor akun GuardDuty administrator yang didelegasikan yang mengelola konfigurasi organisasi.

   Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

   ```
   aws guardduty update-organization-configuration --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
   ```

4. Anda dapat memvalidasi preferensi untuk organisasi Anda di Wilayah saat ini. Jalankan AWS CLI perintah berikut dengan menggunakan ID detektor dari akun GuardDuty administrator yang didelegasikan.

   ```
   aws guardduty describe-organization-configuration --detector-
   id 12abc34d567e8fa901bc2d34e56789f0
   ```

(Disarankan) ulangi langkah sebelumnya di setiap Wilayah dengan menggunakan ID detektor akun GuardDuty administrator yang didelegasikan.

> **Note**
>
> Ketika akun GuardDuty administrator yang didelegasikan memilih keluar dari Wilayah keikutsertaan, meskipun organisasi Anda memiliki konfigurasi GuardDuty aktifkan otomatis yang disetel ke akun anggota baru saja (`NEW`) atau semua akun anggota (`ALL`), GuardDuty tidak dapat diaktifkan untuk akun anggota mana pun di organisasi yang saat

ini telah dinonaktifkan. GuardDuty Untuk informasi tentang konfigurasi akun anggota Anda, buka Akun di panel navigasi GuardDuty konsol atau gunakan ListMembersAPI.

Menambahkan anggota ke organisasi

Sebagai akun GuardDuty administrator yang didelegasikan, Anda dapat menambahkan satu atau lebih Akun AWS ke GuardDuty organisasi. Ketika Anda menambahkan akun sebagai GuardDuty anggota, itu akan secara otomatis GuardDuty diaktifkan di Wilayah itu. Ada pengecualian untuk akun manajemen organisasi. Sebelum akun akun manajemen ditambahkan sebagai GuardDuty anggota, itu harus GuardDuty diaktifkan.

Pilih metode yang disukai untuk menambahkan akun anggota ke GuardDuty organisasi Anda.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Untuk masuk, gunakan kredensyal akun GuardDuty administrator yang didelegasikan.
2. Di panel navigasi, pilih Akun.

   Tabel akun menampilkan semua akun anggota yang aktif (tidak ditangguhkan Akun AWS) dan mungkin terkait dengan akun GuardDuty administrator yang didelegasikan. Jika akun anggota dikaitkan dengan akun administrator organisasi, maka Type akan menjadi salah satu dari yang berikut: Via Organizations or By Invitation. Jika akun anggota tidak terkait dengan akun GuardDuty administrator organisasi, Jenis akun anggota ini bukan anggota.
3. Pilih satu atau beberapa ID akun yang ingin Anda tambahkan sebagai anggota. ID akun ini harus memiliki Type as Via Organizations.

   Akun yang ditambahkan melalui undangan bukan bagian dari organisasi Anda. Anda dapat mengelola akun tersebut secara individual. Untuk informasi selengkapnya, lihat Mengelola akun dengan undangan.
4. Pilih dropdown Tindakan, lalu pilih Tambah anggota. Setelah Anda menambahkan akun ini sebagai anggota, GuardDuty konfigurasi auto-enable akan berlaku. Berdasarkan pengaturan diMenyetel preferensi aktifkan otomatis organisasi, GuardDuty konfigurasi akun ini dapat berubah.

5. Anda dapat memilih panah bawah kolom Status untuk mengurutkan akun berdasarkan status Bukan anggota dan kemudian memilih setiap akun yang belum GuardDuty diaktifkan di Wilayah saat ini.

   Jika tidak ada akun yang tercantum dalam tabel akun yang telah ditambahkan sebagai anggota, Anda dapat mengaktifkan GuardDuty di Wilayah saat ini untuk semua akun organisasi. Pilih Aktifkan di spanduk di bagian atas halaman. Tindakan ini secara otomatis mengaktifkan Auto-enable GuardDuty konfigurasi sehingga GuardDuty diaktifkan untuk setiap akun baru yang bergabung dengan organisasi.
6. Pilih Konfirmasi untuk menambahkan akun sebagai anggota. Tindakan ini juga memungkinkan GuardDuty untuk semua akun yang dipilih. Status akun akan berubah menjadi Diaktifkan.
7. (Disarankan) Ulangi langkah-langkah ini di masing-masing Wilayah AWS. Ini memastikan bahwa akun GuardDuty administrator yang didelegasikan dapat mengelola temuan dan konfigurasi lain untuk akun anggota di semua Wilayah yang telah GuardDuty Anda aktifkan.

   Fitur auto-enable memungkinkan GuardDuty untuk semua anggota masa depan organisasi Anda. Ini memungkinkan akun GuardDuty administrator yang didelegasikan untuk mengelola anggota baru yang dibuat di dalam atau ditambahkan ke organisasi. Ketika jumlah akun anggota mencapai batas 50.000, Auto-enable fitur dimatikan secara otomatis. Jika Anda menghapus akun anggota dan jumlah total anggota berkurang menjadi kurang dari 50.000, Auto-enable fitur akan kembali aktif.

API/CLI

- Jalankan CreateMembersdengan menggunakan kredensi akun administrator yang didelegasikan. GuardDuty

  Anda harus menentukan ID detektor regional dari akun GuardDuty administrator yang didelegasikan dan detail akun (Akun AWS ID dan alamat email yang sesuai) dari akun yang ingin Anda tambahkan sebagai GuardDuty anggota. Anda dapat membuat satu atau beberapa anggota dengan operasi API ini.

  Ketika Anda menjalankan CreateMembers di organisasi Anda, preferensi mengaktifkan otomatis untuk anggota baru akan berlaku saat akun anggota baru bergabung dengan organisasi Anda. Ketika Anda menjalankan CreateMembers dengan akun anggota yang ada,

konfigurasi organisasi juga akan berlaku untuk anggota yang ada. Ini mungkin mengubah konfigurasi akun anggota yang ada saat ini.

Jalankan ListAccountsdi Referensi AWS Organizations API, untuk melihat semua akun di AWS organisasi.

- Atau, Anda dapat menggunakan AWS Command Line Interface. Jalankan AWS CLI perintah berikut dan pastikan untuk menggunakan ID detektor valid Anda sendiri, Akun AWS ID, dan alamat email yang terkait dengan ID akun.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

  ```
  aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
   --account-details AccountId=111122223333,Email=guardduty-member-
  name@amazon.com
  ```

  Anda dapat melihat daftar semua anggota organisasi dengan menjalankan AWS CLI perintah berikut:

  ```
  aws organizations list-accounts
  ```

Setelah Anda menambahkan akun ini sebagai anggota, GuardDuty konfigurasi auto-enable akan berlaku.

(Opsional) Aktifkan paket perlindungan untuk akun anggota yang ada

Prosedur berikut mencakup langkah-langkah untuk mengaktifkan rencana perlindungan untuk akun anggota yang ada dengan menggunakan halaman Akun. Untuk langkah-langkah untuk melakukannya dengan menggunakan API atau AWS CLI, lihat dokumen yang terkait dengan rencana perlindungan tertentu.

Anda dapat mengaktifkan paket perlindungan untuk masing-masing akun melalui halaman Akun.

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Gunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.

3. Pilih satu atau beberapa akun yang ingin Anda konfigurasikan paket perlindungannya. Ulangi langkah-langkah berikut untuk setiap paket perlindungan yang ingin Anda konfigurasi:

   a. Pilih Edit Paket Perlindungan.

   b. Dari daftar rencana perlindungan, pilih satu paket perlindungan yang ingin Anda konfigurasi.

   c. Pilih salah satu tindakan yang ingin Anda lakukan untuk paket perlindungan ini, lalu pilih Konfirmasi.

   d. Untuk akun yang dipilih, kolom yang sesuai dengan paket perlindungan yang dikonfigurasi akan menampilkan konfigurasi yang diperbarui sebagai Diaktifkan atau Tidak diaktifkan.

Terus mengelola akun anggota Anda dalam GuardDuty

Sebagai akun GuardDuty administrator yang didelegasikan, Anda bertanggung jawab untuk menjaga konfigurasi GuardDuty dan rencana perlindungan opsionalnya untuk semua akun di organisasi Anda di setiap yang didukung Wilayah AWS. Bagian berikut memberikan opsi tentang mempertahankan status konfigurasi GuardDuty atau rencana perlindungan opsionalnya:

Untuk mempertahankan status konfigurasi seluruh organisasi Anda di setiap Wilayah

- Setel preferensi aktifkan otomatis untuk seluruh organisasi dengan menggunakan GuardDuty konsol — Anda dapat mengaktifkan GuardDuty secara otomatis untuk semua (`ALL`) anggota dalam organisasi atau anggota baru (`NEW`) yang bergabung dengan organisasi, atau memilih untuk tidak mengaktifkan secara otomatis salah satu anggota dalam organisasi. `NONE`

  Anda juga dapat mengonfigurasi pengaturan yang sama atau berbeda untuk salah satu paket perlindungan di dalamnya GuardDuty.

  Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota di organisasi.

- Perbarui preferensi aktifkan otomatis dengan menggunakan API — Jalankan UpdateOrganizationConfigurationuntuk mengonfigurasi secara otomatis GuardDuty dan rencana perlindungan opsionalnya untuk organisasi. Ketika Anda menjalankan CreateMembersuntuk menambahkan akun anggota baru di organisasi Anda, pengaturan yang dikonfigurasi akan berlaku secara otomatis. Ketika Anda menjalankan CreateMembers dengan akun anggota yang ada, konfigurasi organisasi juga akan berlaku untuk anggota yang ada. Ini mungkin mengubah konfigurasi akun anggota yang ada saat ini.

Untuk melihat semua akun di organisasi Anda, jalankan ListAccountsdi Referensi AWS Organizations API.

Untuk mempertahankan status konfigurasi untuk akun anggota secara individual di setiap Wilayah

- Untuk melihat semua akun di organisasi Anda, jalankan ListAccountsdi Referensi AWS Organizations API.
- Jika Anda ingin akun anggota selektif memiliki status konfigurasi yang berbeda, jalankan UpdateMemberDetectorsuntuk setiap akun anggota satu per satu.

  Anda dapat menggunakan GuardDuty konsol untuk melakukan tugas yang sama dengan menavigasi ke halaman Akun di GuardDuty konsol.

  Untuk informasi tentang mengaktifkan paket perlindungan untuk masing-masing akun dengan menggunakan konsol atau API, lihat halaman konfigurasi untuk paket perlindungan terkait.

Penangguhan GuardDuty untuk akun anggota

Sebagai akun GuardDuty administrator yang didelegasikan, Anda dapat menangguhkan GuardDuty layanan untuk akun anggota di organisasi Anda. Jika Anda melakukan ini, akun anggota tetap berada di GuardDuty organisasi Anda. Anda juga dapat mengaktifkan kembali GuardDuty akun anggota ini di lain waktu. Namun, jika Anda akhirnya ingin memisahkan (menghapus) akun anggota ini, maka setelah mengikuti langkah-langkah di bagian ini, Anda harus mengikuti langkah-langkah diMemutuskan (menghapus) akun anggota dari akun administrator.

Saat Anda menangguhkan GuardDuty akun anggota, Anda dapat mengharapkan perubahan berikut:

- GuardDuty tidak lagi memantau keamanan AWS lingkungan, atau menghasilkan temuan baru.
- Temuan yang ada di akun anggota tetap utuh.
- Akun anggota yang GuardDuty ditangguhkan tidak dikenakan biaya apa pun. GuardDuty

  Jika akun anggota telah mengaktifkan Perlindungan Malware untuk S3 untuk satu atau beberapa bucket di akun mereka, maka penangguhan GuardDuty tidak memengaruhi konfigurasi Perlindungan Malware untuk S3. Akun anggota akan terus menimbulkan biaya penggunaan untuk Perlindungan Malware untuk S3. Agar akun anggota berhenti menggunakan Perlindungan Malware untuk S3, mereka harus menonaktifkan fitur ini untuk ember yang dilindungi. Untuk informasi selengkapnya, lihat Menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi.

Pilih metode yang disukai GuardDuty untuk menangguhkan akun anggota di organisasi Anda.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Untuk masuk, gunakan kredensyal akun administrator yang GuardDuty didelegasikan.
2. Di panel navigasi, pilih Akun.
3. Di halaman Akun, pilih satu atau beberapa akun yang ingin Anda tangguhkan GuardDuty.
4. Pilih menu tarik-turun Tindakan dan kemudian, pilih Tangguhkan. GuardDuty
5. Pilih Tangguhkan GuardDuty untuk mengonfirmasi pilihan.

   Ini akan mengubah Status akun anggota menjadi Dinonaktifkan (ditangguhkan).

   Ulangi langkah sebelumnya di setiap Wilayah tambahan tempat Anda ingin memisahkan atau menghapus akun anggota.

API

1. Untuk mengambil ID akun akun anggota yang ingin ditangguhkan GuardDuty, gunakan API. ListMembers Sertakan `OnlyAssociated` parameter dalam permintaan Anda. Jika Anda menetapkan nilai parameter ini`true`, GuardDuty mengembalikan `members` array yang memberikan rincian tentang hanya akun-akun yang saat ini menjadi GuardDuty anggota.

   Atau, Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk menjalankan perintah berikut:

   ```
   aws guardduty list-members --only-associated true --region us-east-1
   ```

   Ganti *us-east-1* dengan Wilayah tempat Anda ingin menangguhkan GuardDuty akun ini.
2. Untuk menangguhkan satu atau beberapa akun GuardDuty anggota, jalankan StopMonitoringMembersuntuk menangguhkan GuardDuty akun anggota.

   Atau, Anda dapat menggunakan AWS CLI untuk menjalankan perintah berikut:

   ```
   aws guardduty stop-monitoring-members --detector-id
    12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
   ```

Ganti `us-east-1` dengan Wilayah tempat Anda ingin menangguhkan akun ini. Jika Anda memiliki daftar ID akun yang ingin Anda hapus, pisahkan dengan karakter spasi.

Jika Anda ingin memisahkan (menghapus) akun anggota ini, ikuti langkah-langkahnya. Memutuskan (menghapus) akun anggota dari akun administrator

Memutuskan (menghapus) akun anggota dari akun administrator

Saat Anda ingin berhenti mengonfigurasi GuardDuty pengaturan dan mengakses data dari akun anggota, hapus akun itu sebagai akun GuardDuty anggota. Anda dapat melakukannya dengan memisahkan (menghapus) akun itu dari akun GuardDuty administrator.

Ketika Anda memisahkan akun GuardDuty anggota, hal berikut terjadi:

- GuardDuty tetap diaktifkan untuk akun saat ini Wilayah AWS, tetapi akun menjadi terlepas dari akun GuardDuty administrator yang didelegasikan.
- Akun yang terputus terus ditampilkan di inventaris akun.
- Akun GuardDuty administrator tidak lagi memiliki akses ke temuan akun mandiri ini.
- Pemilik akun tidak diberitahu tentang disasosiasi tersebut.

Anda dapat menambahkan akun yang tidak terkait ke organisasi Anda lagi di lain waktu.

Pilih metode yang disukai untuk memisahkan (menghapus) akun anggota dari organisasi Anda.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Untuk masuk, gunakan kredensyal akun administrator yang GuardDuty didelegasikan.
2. Di panel navigasi, pilih Akun.
3. Dalam tabel Akun, Anda dapat menghapus akun yang memiliki Type as Via Organizations and Status as Enabled.

   Pilih satu atau beberapa akun dengan Jenis dan Status yang sama.
4. Dari menu tarik-turun Tindakan, pilih Putuskan akun.
5. Pilih Putuskan akun untuk mengonfirmasi pilihan Anda.

6. Nilai Status untuk akun yang dipilih akan berubah menjadi Bukan anggota. Jumlah Via Organizations (Active/All) di sudut kanan atas halaman Akun akan berubah untuk mencerminkan pembaruan.

   Ulangi langkah sebelumnya di setiap Wilayah tambahan tempat Anda ingin memisahkan akun anggota.

API

1. Untuk mengambil ID akun untuk akun anggota yang ingin Anda hapus, gunakan ListMembersAPI. Sertakan `OnlyAssociated` parameter dalam permintaan Anda. Jika Anda menetapkan nilai parameter ini`true`, GuardDuty mengembalikan `members` array yang memberikan rincian tentang hanya akun-akun yang saat ini menjadi GuardDuty anggota.

   Atau, Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk menjalankan perintah berikut:

   ```
   aws guardduty list-members --only-associated true --region us-east-1
   ```

   Ganti *us-east-1* dengan Wilayah tempat Anda ingin menghapus akun ini.

2. Untuk menghapus satu atau beberapa akun GuardDuty anggota, jalankan DisassociateMembersuntuk menghapus akun anggota yang terkait dengan akun administrator.

   Atau, Anda dapat menggunakan AWS CLI untuk menjalankan perintah berikut:

   ```
   aws guardduty disassociate-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE
    --account-ids 111122223333 --region us-east-1
   ```

   Ganti *us-east-1* dengan Wilayah tempat Anda ingin menghapus akun ini. Jika Anda memiliki daftar ID akun yang ingin Anda hapus, pisahkan dengan karakter spasi.

Menghapus akun anggota dari organisasi GuardDuty

Sebagai akun GuardDuty administrator yang didelegasikan, setelah Anda melepaskan akun anggota dan Anda tidak ingin lagi menyimpan akun anggota tersebut di GuardDuty organisasi, Anda dapat menghapus akun anggota tersebut dari organisasi Anda GuardDuty . Akun anggota ini tidak akan

lagi muncul di inventaris akun Anda. Namun, jika tidak GuardDuty ditangguhkan di akun anggota ini, konfigurasi GuardDuty dan rencana perlindungan khusus tetap sama. Akun ini sekarang akan menjadi akun mandiri dan dapat menonaktifkan GuardDuty diri mereka sendiri.

Langkah ini tidak akan menghapus akun anggota dari AWS organisasi Anda.

Pilih metode yang diinginkan untuk menghapus akun anggota dari GuardDuty organisasi Anda.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Untuk masuk, gunakan kredensyal akun administrator yang GuardDuty didelegasikan.
2. Di panel navigasi, pilih Akun.
3. Dalam tabel Akun, Anda dapat menghapus akun yang memiliki Type as Via Organizations and Status as Removed (disassociated).

   Pilih satu atau beberapa akun dengan Jenis dan Status yang sama.
4. Dari menu tarik-turun Tindakan, pilih Hapus akun.
5. Pilih Hapus akun untuk mengonfirmasi pilihan Anda. Anggota akun yang dipilih tidak akan muncul lagi di tabel Akun Anda.

   Ulangi langkah sebelumnya di setiap Wilayah tambahan tempat Anda ingin menghapus akun anggota ini.

API/CLI

1. Untuk mengambil ID akun untuk akun anggota yang ingin Anda hapus, gunakan ListMembersAPI. Sertakan `OnlyAssociated` parameter dalam permintaan Anda. Jika Anda menetapkan nilai parameter ini`false`, GuardDuty mengembalikan `members` larik yang memberikan rincian hanya tentang akun yang saat ini merupakan GuardDuty anggota yang tidak terkait.

   Atau, Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk menjalankan perintah berikut:

   ```
   aws guardduty list-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --only-associated="false" --region us-east-1
   ```

Ganti *12abc34d567e8fa901bc2d34EXAMPLE* dengan ID detektor akun GuardDuty administrator yang didelegasikan dan *us-east-1* dengan Wilayah tempat Anda ingin menghapus akun ini.

2. Untuk menghapus satu atau beberapa akun GuardDuty anggota, jalankan DeleteMembersuntuk menghapus akun anggota dari GuardDuty organisasi.

   Atau, Anda dapat menggunakan AWS CLI untuk menjalankan perintah berikut:

   ```
   aws guardduty delete-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --
   account-ids 111122223333 --region us-east-1
   ```

   Ganti *12abc34d567e8fa901bc2d34EXAMPLE* dengan ID detektor akun GuardDuty administrator yang didelegasikan dan *us-east-1* dengan Wilayah tempat Anda ingin menghapus akun ini. Jika Anda memiliki daftar ID akun yang ingin Anda hapus, pisahkan dengan karakter spasi.

Mengubah akun GuardDuty administrator yang didelegasikan

Anda dapat menghapus akun GuardDuty administrator yang didelegasikan untuk organisasi Anda di setiap Wilayah dan kemudian mendelegasikan administrator baru di setiap Wilayah. Untuk menjaga postur keamanan akun anggota organisasi Anda di Wilayah, Anda harus memiliki akun GuardDuty administrator yang didelegasikan di Wilayah tersebut.

> **Catatan**
>
> Sebelum menghapus akun GuardDuty administrator yang didelegasikan, Anda harus memisahkan semua akun anggota yang terkait dengan akun GuardDuty administrator yang didelegasikan, lalu menghapusnya dari organisasi. GuardDuty Untuk informasi selengkapnya tentang langkah-langkah ini, lihat dokumen berikut:
>
> - Memutuskan (menghapus) akun anggota dari akun administrator
> - Menghapus akun anggota dari organisasi GuardDuty

Menghapus akun GuardDuty administrator yang didelegasikan

Langkah 1 - Untuk menghapus akun GuardDuty administrator yang didelegasikan yang ada di setiap Wilayah

1. Sebagai akun GuardDuty administrator yang didelegasikan, daftarkan semua akun anggota yang ditautkan dengan akun administrator Anda. Jalankan ListMembersdengan`OnlyAssociated=false`.
2. Jika preferensi aktifkan otomatis untuk GuardDuty atau salah satu paket perlindungan opsional disetel ke`ALL`, jalankan UpdateOrganizationConfigurationuntuk memperbarui konfigurasi organisasi ke salah satu `NEW` atau`NONE`. Tindakan ini akan mencegah kesalahan saat Anda memisahkan semua akun anggota di langkah berikutnya.
3. Jalankan DisassociateMembersuntuk memisahkan semua akun anggota yang terkait dengan akun administrator.
4. Jalankan DeleteMembersuntuk menghapus asosiasi antara akun administrator dan akun anggota.
5. Sebagai akun manajemen organisasi, jalankan DisableOrganizationAdminAccountuntuk menghapus akun GuardDuty administrator yang didelegasikan yang ada.
6. Ulangi langkah-langkah ini di setiap Wilayah AWS tempat Anda memiliki akun GuardDuty administrator yang didelegasikan ini.

Langkah 2 - Untuk membatalkan pendaftaran akun GuardDuty administrator yang didelegasikan yang ada di AWS Organizations (aksi One-time global)

- Jalankan DeregisterDelegatedAdministratordi Referensi AWS Organizations API, untuk membatalkan pendaftaran akun GuardDuty administrator yang sudah didelegasikan. AWS Organizations

  Atau, Anda dapat menjalankan AWS CLI perintah berikut:

  ```
  aws organizations deregister-delegated-administrator --account-id 111122223333 --
  service-principal guardduty.amazonaws.com
  ```

  Pastikan untuk mengganti *111122223333* dengan akun GuardDuty administrator yang didelegasikan yang ada.

Setelah Anda membatalkan pendaftaran akun GuardDuty administrator lama yang didelegasikan, Anda dapat menambahkannya sebagai akun anggota ke akun administrator yang didelegasikan GuardDuty baru.

Menunjuk akun GuardDuty administrator baru yang didelegasikan di setiap Wilayah

1. Tentukan akun GuardDuty administrator baru yang didelegasikan di setiap Wilayah dengan menggunakan metode akses pilihan Anda - GuardDuty konsol, atau API atau. AWS CLI Untuk informasi selengkapnya, lihat Menunjuk akun administrator yang didelegasikan GuardDuty.
2. Jalankan DescribeOrganizationConfigurationuntuk melihat konfigurasi aktifkan otomatis saat ini untuk organisasi Anda.

> **Important**
>
> Sebelum menambahkan anggota ke akun GuardDuty administrator yang didelegasikan baru, Anda harus memverifikasi konfigurasi aktifkan otomatis untuk organisasi Anda. Konfigurasi ini khusus untuk akun GuardDuty administrator yang didelegasikan baru dan Wilayah yang dipilih, dan tidak terkait AWS Organizations dengan. Saat Anda menambahkan akun anggota organisasi (baru atau yang sudah ada) di bawah akun GuardDuty administrator yang didelegasikan baru, konfigurasi aktifkan otomatis akun GuardDuty administrator yang didelegasikan akan berlaku pada saat mengaktifkan GuardDuty atau salah satu paket perlindungan opsionalnya.

Ubah konfigurasi organisasi untuk akun GuardDuty administrator baru yang didelegasikan dengan menggunakan metode akses pilihan Anda - GuardDuty konsol, atau API atau AWS CLI. Lihat informasi yang lebih lengkap di Menyetel preferensi aktifkan otomatis organisasi.

Mengelola akun menggunakan kebijakan organisasi

Kebijakan GuardDuty organisasi memungkinkan Anda mengaktifkan dan mengelola Amazon secara terpusat GuardDuty di seluruh akun di organisasi Anda. Anda menggunakan kebijakan AWS Organizations deklaratif untuk menentukan entitas organisasi mana (root organisasi, unit organisasi (OU), atau akun individual) yang memiliki detektor GuardDuty dasar dan rencana perlindungannya secara otomatis diaktifkan dan dikelola melalui akun administrator yang didelegasikan GuardDuty .

Akun yang bergabung dengan organisasi, atau pindah ke OU yang memiliki kebijakan terlampir, mewarisi kebijakan dan memiliki GuardDuty dan rencana perlindungannya dikonfigurasi sesuai dengan apa yang didefinisikan oleh kebijakan efektif untuk mereka.

GuardDuty kebijakan organisasi adalah mekanisme yang berbeda dari pengaturan aktifkan otomatis yang dijelaskan dalamMengelola GuardDuty akun dengan AWS Organizations. Untuk konsep kebijakan, struktur, pewarisan, validasi, dan kebijakan contoh, lihat GuardDutykebijakan di AWS Organizations Panduan Pengguna.

Daftar Isi

- Prasyarat
- Bagaimana kebijakan organisasi bekerja
- Membuat kebijakan di konsol
- Meninjau dampak kebijakan sebelum Anda menerapkannya
- Pertimbangan dan batasan

Prasyarat

Sebelum Anda menggunakan kebijakan GuardDuty organisasi, lengkapi prasyarat berikut:

- Aktifkan akses tepercaya untuk GuardDuty layanan di AWS Organizations.
- Tetapkan akun GuardDuty administrator yang didelegasikan.
- Lampirkan kebijakan delegasi yang memberikan izin administrator yang didelegasikan untuk mengelola kebijakan. GuardDuty
- Aktifkan jenis `GUARDDUTY_POLICY` kebijakan di root organisasi. Ini terjadi secara otomatis ketika administrator yang didelegasikan membuat kebijakan pertama di GuardDuty konsol.

> **Warning**
>
> Mengaktifkan jenis `GUARDDUTY_POLICY` kebijakan akan menghentikan penerapan pengaturan GuardDuty pengaktifan otomatis Regional, bahkan sebelum Anda melampirkan kebijakan. Karena konsol mengaktifkan jenis kebijakan ini secara otomatis saat administrator yang didelegasikan membuat kebijakan pertama, Anda dapat berhenti mengandalkan pengaktifan otomatis tanpa bermaksud melakukannya. Tinjau konfigurasi pengaktifan otomatis yang ada sebelum membuat kebijakan pertama.

Untuk langkah-langkah terperinci, lihat GuardDutykebijakan di Panduan AWS Organizations Pengguna.

Bagaimana kebijakan organisasi bekerja

Kebijakan GuardDuty organisasi menentukan GuardDuty fitur mana yang diaktifkan, di Wilayah mana, dan untuk akun mana. Bagian berikut menjelaskan bagaimana kebijakan berlaku di seluruh Wilayah, cara kebijakan diwarisi melalui organisasi Anda, cara kebijakan aktif mengubah cara Anda mengelola GuardDuty akun, dan cara umum untuk menggunakan kebijakan.

Daftar Isi

- Konfigurasi regional
- Warisan kebijakan dan prioritas
- Bagaimana kebijakan memengaruhi manajemen GuardDuty akun
- Contoh kasus penggunaan

Konfigurasi regional

Kebijakan GuardDuty organisasi menetapkan pemberdayaan per Wilayah. Konfigurasi default berlaku di setiap Wilayah GuardDuty jika tersedia. Anda dapat menambahkan penggantian Regional untuk memberikan konfigurasi yang berbeda pada Wilayah tertentu. Konfigurasi default adalah opsional. Jika Anda menghilangkannya, hanya Wilayah yang Anda tentukan yang dikelola, dan setiap Wilayah lainnya dibiarkan tidak terkelola.

Jika kebijakan diaktifkan GuardDuty secara luas, seperti konfigurasi default yang mencakup setiap Wilayah, akan GuardDuty memproses peristiwa layanan AWS CloudTrail global di setiap Wilayah yang diaktifkan, termasuk Wilayah di mana Anda tidak memiliki sumber daya atau beban kerja. Untuk informasi selengkapnya, lihat Bagaimana GuardDuty menangani AWS CloudTrail peristiwa global.

Kebijakan mengelola GuardDuty dan rencana perlindungan hanya di Wilayah di mana mereka tersedia. Jika kebijakan Anda mengaktifkan GuardDuty atau rencana perlindungan di Wilayah yang tidak tersedia, kebijakan akan melewatinya di Wilayah tersebut tanpa kesalahan. Sebelum Anda mengonfigurasi kebijakan, tinjau di mana GuardDuty dan setiap paket perlindungan tersedia. Untuk informasi selengkapnya, lihat Region-specific ketersediaan fitur.

Penggantian Regional sepenuhnya menggantikan konfigurasi default untuk Wilayah tersebut. Itu tidak bergabung dengan default, jadi Anda harus menentukan setiap paket perlindungan yang ingin

Anda kelola di Wilayah itu. Paket perlindungan apa pun yang Anda tinggalkan dari penggantian tidak dikelola di Wilayah itu, meskipun konfigurasi default mengelolanya. Karena itu, rencana perlindungan yang dikelola kebijakan dapat berbeda dari satu Wilayah ke Wilayah berikutnya.

Untuk struktur kebijakan lengkap dan bagaimana Wilayah diselesaikan, lihat GuardDuty kebijakan di Panduan AWS Organizations Pengguna.

Warisan kebijakan dan prioritas

GuardDuty Kebijakan organisasi mengikuti model AWS Organizations pewarisan. Kebijakan yang dilampirkan di root organisasi berlaku untuk setiap akun di organisasi. Akun juga mewarisi kebijakan apa pun yang dilampirkan pada OU induk. Ketika lebih dari satu kebijakan berlaku untuk akun, AWS Organizations gabungkan mereka ke dalam satu kebijakan yang efektif, dan kebijakan yang dilampirkan lebih dekat ke akun lebih diutamakan daripada kebijakan yang dilampirkan lebih tinggi dalam hierarki.

Setelah mengaktifkan jenis `GUARDDUTY_POLICY` kebijakan, kebijakan akan diutamakan daripada pengaturan pengaktifan GuardDuty otomatis Regional. Pengaturan pengaktifan otomatis tidak lagi berlaku, terlepas dari apakah kebijakan dilampirkan atau tidak.

Untuk mengetahui aturan pewarisan lengkap dan bagaimana kebijakan yang efektif diselesaikan, lihat Memahami pewarisan kebijakan manajemen di AWS Organizations Panduan Pengguna.

Bagaimana kebijakan memengaruhi manajemen GuardDuty akun

Saat kebijakan GuardDuty organisasi aktif, perubahan berikut berlaku untuk cara Anda mengelola GuardDuty akun:

- Setelah jenis `GUARDDUTY_POLICY` kebijakan diaktifkan, pengaturan GuardDuty pengaktifan otomatis Regional tidak lagi berlaku, terlepas dari apakah kebijakan dilampirkan atau tidak.
- Saat kebijakan mengelola rencana perlindungan, rencana perlindungan tersebut tidak dapat lagi diubah melalui GuardDuty konsol atau API untuk akun yang tercakup. Pada halaman Akun muncul sebagai Kebijakan dikelola. Untuk mengubah rencana perlindungan terkelola, perbarui kebijakan. Paket perlindungan yang tidak dikelola kebijakan tetap dapat diedit melalui konsol dan API.
- Hanya akun administrator yang didelegasikan yang dapat membuat dan mengelola GuardDuty kebijakan. Halaman kebijakan Organisasi di GuardDuty konsol hanya tersedia untuk administrator yang didelegasikan.

> **Note**
>
> Melampirkan GuardDuty kebijakan dapat mendaftarkan akun baru sebagai GuardDuty anggota dan mengaktifkan rencana perlindungan di seluruh organisasi Anda. Mengaktifkan GuardDuty dan rencana perlindungannya menimbulkan biaya. Untuk informasi selengkapnya, lihat Harga di GuardDuty.

Contoh kasus penggunaan

Contoh berikut menunjukkan cara umum untuk menggunakan kebijakan GuardDuty organisasi. Untuk JSON kebijakan yang mengimplementasikan setiap pola, lihat GuardDuty kebijakan di AWS Organizations Panduan Pengguna.

- Aktifkan baseline perlindungan di seluruh organisasi. Lampirkan kebijakan di root organisasi dengan konfigurasi default yang memungkinkan detektor dasar dan rencana perlindungan yang Anda butuhkan. Setiap akun, termasuk akun yang bergabung nanti, mengaktifkan fitur tersebut secara otomatis.
- Perlindungan bervariasi menurut unit organisasi. Gunakan kebijakan luas di root untuk baseline Anda, dan lampirkan kebijakan yang lebih spesifik ke masing-masing OU untuk menyesuaikan rencana perlindungan akun dengan persyaratan kepatuhan atau beban kerja yang berbeda.
- Pertahankan cakupan saat organisasi Anda tumbuh. Karena akun yang bergabung dengan organisasi atau pindah ke OU tertutup mewarisi kebijakan yang efektif, kebijakan membuat akun yang baru dibuat selaras dengan garis dasar perlindungan Anda tanpa pengaktifan manual.

Membuat kebijakan di konsol

Anda membuat dan mengelola GuardDuty kebijakan dari akun administrator yang didelegasikan, di halaman Kebijakan organisasi di GuardDuty konsol. Membuat kebijakan pertama Anda juga memungkinkan jenis `GUARDDUTY_POLICY` kebijakan untuk organisasi Anda secara otomatis.

Untuk membuat GuardDuty kebijakan

1. Masuk ke GuardDuty konsol dengan akun administrator yang didelegasikan.
2. Di panel navigasi, pilih Kebijakan organisasi, lalu pilih Buat kebijakan.
3. Untuk Langkah 1: Detail kebijakan, masukkan nama kebijakan dan deskripsi opsional, lalu pilih Berikutnya.

4. Untuk Langkah 2: Akun, pilih tempat kebijakan dilampirkan dalam hierarki organisasi Anda, lalu pilih Berikutnya:
   - Semua unit dan akun organisasi melampirkan kebijakan di seluruh organisasi.
   - Unit dan akun organisasi tertentu melampirkannya ke entitas yang Anda pilih.
   - Tidak ada unit organisasi atau akun yang membuat kebijakan tanpa melampirkannya.
5. Untuk Langkah 3: Detail konfigurasi, di bawah Pemilihan kemampuan, pilih rencana perlindungan yang dikelola kebijakan ini. Gunakan Aktifkan semua atau Nonaktifkan semua untuk titik awal yang cepat, lalu sesuaikan rencana perlindungan individu. Paket perlindungan yang tidak Anda pilih tidak terpengaruh oleh kebijakan ini. Deteksi ancaman dasar harus diaktifkan jika Anda mengaktifkan rencana perlindungan lainnya. Pilih Berikutnya.
6. (Opsional) Untuk Langkah 4: Penggantian regional, pilih Tambahkan penggantian regional, pilih satu atau beberapa Wilayah, dan atur konfigurasi untuk Wilayah tersebut. Penggantian regional sepenuhnya menggantikan konfigurasi default untuk Wilayah, jadi tentukan setiap paket perlindungan yang ingin Anda kelola di sana. Pilih Berikutnya.
7. Untuk Langkah 5: Tinjau dan buat, tinjau detail kebijakan, akun, konfigurasi default, dan penggantian Regional apa pun. Untuk melihat JSON kebijakan yang dihasilkan, perluas dokumen Kebijakan. Kemudian pilih Buat kebijakan.

Anda dapat meninjau atau mengedit JSON yang dihasilkan pada langkah apa pun dengan memperluas dokumen Kebijakan. Untuk struktur kebijakan, aturan pewarisan, dan contoh kebijakan, lihat GuardDutykebijakan di Panduan AWS Organizations Pengguna.

Meninjau dampak kebijakan sebelum Anda menerapkannya

Sebelum Anda menyimpan perubahan kebijakan yang menonaktifkan rencana perlindungan, tinjau akun dan Wilayah mana yang saat ini mengaktifkan paket perlindungan tersebut, sehingga Anda memahami perubahan apa yang akan dimatikan. Karena GuardDuty kebijakan berlaku per Wilayah, periksa status pemberdayaan saat ini per akun dan per Wilayah.

> **Warning**
>
> Kebijakan yang menonaktifkan GuardDuty atau rencana perlindungan mematikannya di setiap akun tertutup yang saat ini diaktifkan, dan mencegah akun tersebut menyalakannya kembali melalui konsol atau API. Anda dapat secara tidak sengaja menonaktifkan perlindungan yang diandalkan akun. Sebelum Anda membuat atau memperbarui kebijakan,

identifikasi akun dan Wilayah yang dipengaruhi perubahan, seperti yang dijelaskan di bagian ini, dan konfirmasikan dampak yang dimaksudkan.

Sebagai administrator yang didelegasikan, Anda dapat meninjau GuardDuty pemberdayaan saat ini di seluruh organisasi menggunakan halaman Akun GuardDuty konsol (alihkan Wilayah untuk meninjau cakupan di setiap Wilayah), atau secara terprogram dengan langkah-langkah berikut. Lakukan langkah-langkah API di setiap Wilayah yang ingin Anda tinjau.

Untuk mengidentifikasi akun dan Wilayah yang dipengaruhi oleh kebijakan

1. Hitung akun di organisasi Anda. Gunakan operasi AWS Organizations `ListAccounts` API untuk mencantumkan setiap akun di organisasi, termasuk akun yang belum menjadi GuardDuty anggota.
2. Hitung akun anggota Anda GuardDuty . Gunakan operasi GuardDuty `ListMembers` API untuk membuat daftar akun yang sudah menjadi akun GuardDuty anggota.
3. Tinjau paket perlindungan yang diaktifkan untuk setiap akun anggota. Gunakan operasi GuardDuty `GetMemberDetectors` API untuk melihat fitur mana yang diaktifkan untuk setiap detektor akun anggota.
4. Bandingkan pemberdayaan saat ini dengan rencana perlindungan yang akan dinonaktifkan oleh perubahan kebijakan Anda untuk mengidentifikasi akun dan Wilayah yang dipengaruhi perubahan tersebut.

Akun milik organisasi Anda tetapi belum GuardDuty menjadi anggota tidak muncul`ListMembers`, dan Anda tidak dapat melihat status detektornya sampai Anda menambahkannya sebagai anggota. Ketika GuardDuty kebijakan berlaku untuk akun yang belum menjadi anggota, akun tersebut secara otomatis ditambahkan sebagai anggota.

Setelah Anda membuat dan melampirkan kebijakan, konfirmasikan kebijakan final yang berlaku untuk akun tertentu. Kebijakan efektif adalah agregasi dari setiap kebijakan yang diwarisi akun dari entitas induknya, dikombinasikan dengan kebijakan apa pun yang dilampirkan langsung ke akun. Untuk melihatnya, gunakan operasi AWS Organizations `DescribeEffectivePolicy` API, atau setara AWS CLI atau AWS SDK, dengan tipe kebijakan. GuardDuty Akun apa pun dengan izin untuk memanggil operasi ini dapat menggunakannya, termasuk akun administrator yang didelegasikan. Untuk informasi selengkapnya, lihat Melihat kebijakan deklaratif yang efektif di Panduan AWS Organizations Pengguna.

Pertimbangan dan batasan

Ingatlah hal-hal berikut ketika Anda merencanakan dan mengelola kebijakan GuardDuty organisasi:

- Kebijakan hanya berlaku untuk akun di AWS Organizations. Kebijakan organisasi GuardDuty hanya dapat dikelola di akun milik organisasi Anda AWS Organizations. Itu tidak dapat mengelola akun yang bukan bagian dari organisasi Anda, seperti akun yang hanya terkait dengan metode undangan lama. Kelola akun tersebut GuardDuty secara terpisah, dari akun akun GuardDuty administrator yang didelegasikan atau di setiap akun. Untuk informasi lebih lanjut tentang dua metode asosiasi, lihatMengelola banyak akun di Amazon GuardDuty.
- Kebijakan dapat diaktifkan GuardDuty di akun manajemen hanya jika peran terkait layanan sudah ada di sana. Kebijakan tidak dapat diaktifkan GuardDuty di akun manajemen organisasi kecuali peran GuardDuty terkait layanan sudah ada di akun tersebut. Jika peran tidak ada, tidak GuardDuty diaktifkan di akun manajemen meskipun kebijakan mendeklarasikannya diaktifkan. Buat peran di akun manajemen, misalnya dengan mengaktifkan di GuardDuty sana, sebelum Anda mengandalkan kebijakan untuk mengelolanya.
- Administrator yang didelegasikan ditetapkan per Wilayah, dan mengaktifkan akun terpisah dari melihatnya. Akun manajemen menunjuk administrator yang GuardDuty didelegasikan di setiap Wilayah. Administrator yang didelegasikan yang ditetapkan di satu Wilayah dapat membuat kebijakan yang memungkinkan GuardDuty akun anggota, termasuk di Wilayah yang bukan administrator yang didelegasikan. Namun, administrator yang didelegasikan tidak dapat melihat status atau temuan akun anggota tersebut di Wilayah kecuali akun manajemen juga telah menetapkannya sebagai administrator yang didelegasikan di Wilayah tersebut. Untuk mengelola dan memantau akun anggota di Wilayah, akun manajemen harus menunjuk administrator yang didelegasikan di Wilayah tersebut. Karena penunjukan adalah per Wilayah, akun manajemen dapat menunjuk akun yang berbeda sebagai administrator yang didelegasikan di Wilayah yang berbeda, dan setiap administrator yang didelegasikan mengelola dan memantau akun anggota hanya di Wilayah yang ditunjuk.
- Administrator yang didelegasikan memerlukan kebijakan AWS Organizations delegasi untuk mengelola kebijakan. Menunjuk administrator yang didelegasikan memungkinkannya melihat akun anggota, tetapi tidak dapat membuat, memperbarui, atau melampirkan kebijakan GuardDuty organisasi kecuali kebijakan AWS Organizations delegasi juga memberinya izin untuk mengelola jenis kebijakan. `GUARDDUTY_POLICY` Jika operasi tersebut ditolak, verifikasi bahwa kebijakan delegasi memberikan izin administrator yang didelegasikan untuk mengelola jenis kebijakan.
- Paket perlindungan terkelola hanya bisa dibaca di konsol dan API. Saat kebijakan mengelola rencana perlindungan, akun yang tercakup tidak dapat mengubahnya melalui GuardDuty konsol

atau API. Untuk mengubah rencana perlindungan terkelola, perbarui kebijakan. Paket perlindungan yang tidak dikelola kebijakan tetap dapat diedit melalui konsol dan API.

- Kebijakan hanya mengelola pemberdayaan, bukan penyesuaian deteksi. Kebijakan GuardDuty organisasi memungkinkan dan menonaktifkan GuardDuty dan rencana perlindungannya. Itu tidak mengelola kustomisasi deteksi seperti daftar entitas, daftar alamat IP, atau aturan penindasan. Konfigurasikan ini secara terpisah melalui GuardDuty konsol atau API setelah GuardDuty diaktifkan. Untuk informasi selengkapnya, lihat Menyesuaikan deteksi ancaman dengan daftar entitas dan daftar alamat IP dan Aturan penindasan di GuardDuty.
- Wilayah yang tidak dikelola dibiarkan tidak berubah, tidak dinonaktifkan. Wilayah yang tidak disertakan kebijakan dalam konfigurasi default maupun nama dalam penggantian Regional tidak dikelola. Kebijakan tidak mengaktifkan atau menonaktifkan GuardDuty di sana, dan pengaturan yang ada di Wilayah tersebut dibiarkan apa adanya.
- GuardDuty memproses peristiwa global di setiap Wilayah yang diaktifkan. GuardDuty mereplikasi peristiwa layanan AWS CloudTrail global, dari layanan seperti IAM, Amazon S3 AWS STS, dan Amazon, dan memprosesnya di setiap Wilayah yang diaktifkan, termasuk Wilayah GuardDuty di mana Anda tidak memiliki sumber daya atau beban kerja. CloudFront Ini meningkatkan deteksi ancaman, tetapi ini berarti bahwa ketika kebijakan memungkinkan GuardDuty secara luas, seperti konfigurasi default yang mencakup setiap Wilayah, GuardDuty memproses peristiwa global ini di semua Wilayah tersebut, yang dapat menimbulkan biaya tambahan GuardDuty . Untuk informasi selengkapnya, lihat Bagaimana GuardDuty menangani AWS CloudTrail peristiwa global dan Harga di GuardDuty.
- Menonaktifkan paket perlindungan mematikannya di tempat yang saat ini diaktifkan. Kebijakan yang menonaktifkan GuardDuty atau rencana perlindungan mematikannya di setiap akun tertutup yang diaktifkan, dan mencegah akun tersebut menyalakannya kembali melalui konsol atau API. Sebelum Anda membuat atau memperbarui kebijakan, identifikasi akun dan Wilayah yang dipengaruhi perubahan, seperti yang dijelaskan dalamMeninjau dampak kebijakan sebelum Anda menerapkannya.
- Perubahan kebijakan berlaku secara asinkron. Perubahan kebijakan menyebar ke seluruh organisasi Anda dan direkonsiliasi dari waktu ke waktu, daripada berlaku secara instan. Berikan waktu untuk perubahan untuk diterapkan sebelum Anda menyimpulkan bahwa itu tidak berlaku.
- Melepaskan kebijakan tidak menonaktifkan GuardDuty. Saat Anda melepaskan kebijakan GuardDuty organisasi dari entitas, kebijakan lain yang diwarisi entitas dari entitas induk masih dapat berlaku dan terus mengatur target. Jika tidak ada kebijakan efektif yang tersisa setelah Anda melepaskan, GuardDuty dan rencana perlindungannya tetap dalam keadaan saat ini dan tidak dinonaktifkan. Dalam kedua kasus tersebut, perubahan future pada organisasi Anda, seperti akun

baru yang bergabung atau akun yang sudah ada pindah ke OU, tidak lagi diaktifkan GuardDuty secara otomatis kecuali kebijakan yang diwariskan masih mencakupnya. Pemberdayaan lebih lanjut harus dilakukan secara manual, dengan melampirkan kembali kebijakan, atau melalui kebijakan yang diwariskan.

- Menonaktifkan jenis kebijakan menghentikan semua manajemen kebijakan dan memulihkan pengaktifan otomatis. Menonaktifkan GuardDuty kebijakan, melepaskan kebijakan, dan menonaktifkan jenis `GUARDDUTY_POLICY` kebijakan adalah tiga tindakan berbeda dengan efek berbeda. Saat Anda menonaktifkan jenis `GUARDDUTY_POLICY` kebijakan di root organisasi, kebijakan GuardDuty organisasi tidak lagi mengatur akun apa pun, dan GuardDuty tetap diaktifkan di akun yang dicakup sebelumnya. Menonaktifkan jenis kebijakan juga memulihkan pengaturan GuardDuty pengaktifan otomatis Regional yang telah ditekan oleh mengaktifkan jenis kebijakan, sehingga pengaktifan otomatis dilanjutkan sesuai dengan setelan tersebut.

Mengelola GuardDuty akun dengan undangan

Untuk mengelola akun di luar organisasi, Anda dapat menggunakan metode undangan lawas. Jika Anda menggunakan metode ini, akun Anda ditetapkan sebagai akun administrator saat akun lain menerima undangan Anda untuk menjadi akun anggota.

> **Note**
>
> GuardDuty merekomendasikan menggunakan AWS Organizations alih-alih GuardDuty undangan, untuk mengelola akun anggota Anda. Untuk informasi selengkapnya, lihat Mengelola akun dengan AWS Organizations.

Jika akun Anda bukan akun administrator, Anda dapat menerima undangan dari akun lain. Jika Anda menerima, akun Anda menjadi akun anggota. AWS Akun tidak dapat berupa akun GuardDuty administrator dan akun anggota secara bersamaan.

Ketika Anda menerima undangan dari satu akun, Anda tidak dapat menerima undangan dari akun lain. Untuk menerima undangan dari akun lain, Anda harus terlebih dahulu memisahkan akun Anda dari akun administrator yang ada. Atau, akun administrator juga dapat memisahkan dan menghapus akun Anda dari organisasi mereka.

Akun yang terkait dengan undangan memiliki hubungan akun-ke-anggota administrator keseluruhan yang serupa dengan akun yang terkait dengan AWS Organizations, seperti yang dijelaskan dalam.

Memahami hubungan antara akun GuardDuty administrator dan akun anggota Namun, pengguna akun administrator undangan tidak dapat mengaktifkan GuardDuty atas nama akun anggota terkait atau melihat akun non-anggota lainnya dalam AWS Organizations organisasi mereka.

> **Important**
>
> Cross-regional transfer data dapat terjadi ketika GuardDuty membuat akun anggota menggunakan metode ini. Untuk memverifikasi alamat email akun anggota, GuardDuty gunakan layanan verifikasi email yang hanya beroperasi di Wilayah AS Timur (Virginia N.).

Topik

- Menambahkan akun dengan undangan
- Mengkonsolidasikan akun GuardDuty administrator di bawah satu organisasi

Menambahkan akun dengan undangan

Sebagai akun administrator yang telah GuardDuty diaktifkan, Anda dapat menambahkan anggota untuk mulai menggunakan GuardDuty. Setelah menambahkan anggota, Anda dapat mengundang mereka untuk bergabung GuardDuty, dan mereka dapat memilih untuk menanggapi undangan Anda.

> **Note**
>
> GuardDuty merekomendasikan menggunakan AWS Organizations alih-alih GuardDuty undangan, untuk mengelola akun anggota Anda. Untuk informasi selengkapnya, lihat Mengelola akun dengan AWS Organizations.

Pilih metode akses yang disukai untuk menambahkan akun GuardDuty anggota sebagai akun GuardDuty administrator.

Console

Langkah 1 - Tambahkan akun

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Akun.

3. Pilih Tambahkan akun berdasarkan undangan di panel atas.
4. Pada halaman Tambahkan akun anggota, di bawah Masukkan detail akun, masukkan Akun AWS ID dan alamat email yang terkait dengan akun yang ingin Anda tambahkan.
5. Untuk menambahkan baris lain untuk memasukkan detail akun satu per satu, pilih Tambahkan akun lain. Anda juga dapat memilih Unggah file.csv dengan detail akun untuk menambahkan akun secara massal.

   > **Important**
   >
   > Baris pertama file csv Anda harus berisi header, seperti yang digambarkan dalam contoh berikut —. `Account ID,Email` Setiap baris berikutnya harus berisi satu Akun AWS ID yang valid dan alamat email yang terkait. Format baris valid jika hanya berisi satu Akun AWS ID dan alamat email terkait dipisahkan oleh koma.
   >
   > ```
   > Account ID,Email
   >                                 555555555555,user@example.com
   > ```

6. Setelah Anda menambahkan semua detail akun, pilih Berikutnya. Anda dapat melihat akun yang baru ditambahkan di tabel Akun. Status akun ini akan menjadi Undangan tidak terkirim. Untuk informasi tentang mengirim undangan ke satu atau beberapa akun tambahan, lihatStep 2 - Invite an account.

Langkah 2 - Undang akun

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Akun.
3. Pilih satu atau beberapa akun yang ingin Anda undang ke Amazon GuardDuty.
4. Pilih menu tarik-turun Tindakan dan kemudian pilih Undang.
5. Di kotak GuardDuty dialog Undangan ke, masukkan pesan undangan (opsional).

   Jika akun yang diundang tidak memiliki akses ke email, pilih kotak centang Juga kirim pemberitahuan email ke pengguna root pada undangan Akun AWS dan buat peringatan di undangan. Dasbor AWS Health
6. Pilih Kirim undangan. Jika undangan memiliki akses ke alamat email yang ditentukan, mereka dapat melihat undangan dengan membuka GuardDuty konsol di. https://console.aws.amazon.com/guardduty/

7. Saat undangan menerima undangan, nilai di kolom Status berubah menjadi Diundang. Untuk informasi tentang menerima undangan, lihatStep 3 - Accept an invitation.

Langkah 3 - Terima undangan

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   > **Important**
   >
   > Anda harus mengaktifkan GuardDuty sebelum Anda dapat melihat atau menerima undangan keanggotaan.

2. Lakukan hal berikut hanya jika Anda GuardDuty belum mengaktifkan; jika tidak, Anda dapat melewati langkah ini dan melanjutkan dengan langkah berikutnya.

   Jika Anda belum mengaktifkan GuardDuty, pilih Memulai di GuardDuty halaman Amazon.

   Pada GuardDuty halaman Selamat Datang di, pilih Aktifkan GuardDuty.

3. Setelah mengaktifkan GuardDuty akun Anda, gunakan langkah-langkah berikut untuk menerima undangan keanggotaan:

   a. Pada panel navigasi, silakan pilih Pengaturan.

   b. Pilih Akun .

   c. Pada Akun, pastikan untuk memverifikasi pemilik akun tempat Anda menerima undangan. Aktifkan Terima untuk menerima undangan keanggotaan.

4. Setelah Anda menerima undangan, akun Anda menjadi akun GuardDuty anggota. Akun yang pemiliknya mengirim undangan menjadi akun GuardDuty administrator. Akun administrator akan tahu bahwa Anda telah menerima undangan. Tabel Akun di GuardDuty akun mereka akan diperbarui. Nilai di kolom Status yang sesuai dengan ID akun anggota Anda akan berubah menjadi Diaktifkan. Pemilik akun administrator sekarang dapat melihat GuardDuty dan mengelola serta konfigurasi paket perlindungan atas nama akun Anda. Akun administrator juga dapat melihat dan mengelola GuardDuty temuan yang dihasilkan untuk akun anggota Anda.

API/CLI

Anda dapat menunjuk akun GuardDuty administrator, dan membuat atau menambahkan akun GuardDuty anggota dengan undangan melalui operasi API. Jalankan operasi GuardDuty API berikut untuk menetapkan akun administrator dan akun anggota. GuardDuty

Selesaikan prosedur berikut menggunakan kredensi Akun AWS yang ingin Anda tetapkan sebagai akun administrator. GuardDuty

Membuat atau menambahkan akun anggota

1. Jalankan operasi CreateMembersAPI menggunakan kredensional AWS akun yang telah GuardDuty diaktifkan. Ini adalah akun yang Anda inginkan menjadi akun GuardDuty akun administrator.

   Anda harus menentukan ID detektor AWS akun saat ini dan ID akun serta alamat email dari akun yang ingin Anda jadikan GuardDuty anggota. Anda dapat membuat satu atau beberapa anggota dengan operasi API ini.

   Anda juga dapat menggunakan AWS Command Line Tools untuk menunjuk akun administrator dengan menjalankan perintah CLI berikut. Pastikan untuk menggunakan ID pendeteksi, ID akun, dan email Anda sendiri yang valid.

   Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=111122223333,Email=guardduty-member@organization.com
   ```

2. Jalankan InviteMembersdengan menggunakan kredensi AWS akun yang telah GuardDuty diaktifkan. Ini adalah akun yang Anda inginkan menjadi akun GuardDuty akun administrator.

   Anda harus menentukan ID detektor AWS akun saat ini dan ID akun akun yang ingin Anda jadikan GuardDuty anggota. Anda dapat mengundang satu anggota atau lebih dengan operasi API ini.

   > **Note**
   >
   > Anda juga dapat menentukan pesan undangan opsional dengan menggunakan parameter `message` permintaan.

Anda juga dapat menggunakan AWS Command Line Interface untuk menunjuk akun anggota dengan menjalankan perintah berikut. Pastikan untuk menggunakan ID detektor yang valid dan ID akun yang valid untuk akun yang ingin Anda undang.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 111122223333
```

Menerima undangan

Selesaikan prosedur berikut menggunakan kredensi dari setiap AWS akun yang ingin Anda tetapkan sebagai GuardDuty akun anggota.

1. Jalankan operasi CreateDetectorAPI untuk setiap AWS akun yang diundang untuk menjadi akun GuardDuty anggota dan Anda ingin menerima undangan.

   Anda harus menentukan apakah sumber daya detektor akan diaktifkan menggunakan GuardDuty layanan. Detektor harus dibuat dan diaktifkan GuardDuty agar dapat beroperasi. Anda harus mengaktifkan terlebih dahulu GuardDuty sebelum menerima undangan.

   Anda juga dapat melakukan ini dengan menggunakan AWS Command Line Tools menggunakan perintah CLI berikut.

   ```
   aws guardduty create-detector --enable
   ```

2. Jalankan operasi AcceptAdministratorInvitationAPI untuk setiap AWS akun yang ingin Anda terima undangan keanggotaan, menggunakan kredensi akun tersebut.

   Anda harus menentukan ID detektor AWS akun ini untuk akun anggota, ID akun akun administrator yang mengirim undangan, dan ID undangan undangan yang Anda terima. Anda dapat menemukan ID akun administrator di email undangan atau dengan menggunakan operasi API ListInvitations.

   Anda juga dapat menerima undangan menggunakan AWS Command Line Tools dengan menjalankan perintah CLI berikut. Pastikan Anda menggunakan ID detektor, ID akun administrator, dan ID undangan yang valid.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --administrator-id 444455556666 --invitation-
id 84b097800250d17d1872b34c4daadcf5
```

Mengkonsolidasikan akun GuardDuty administrator di bawah satu organisasi

GuardDuty merekomendasikan penggunaan asosiasi melalui AWS Organizations untuk mengelola akun anggota di bawah akun GuardDuty administrator yang didelegasikan. Anda dapat menggunakan contoh proses yang diuraikan di bawah ini untuk mengkonsolidasikan akun administrator dan anggota yang terkait dengan undangan dalam organisasi di bawah satu akun administrator yang GuardDuty didelegasikan GuardDuty .

> **Note**
>
> GuardDuty merekomendasikan menggunakan AWS Organizations alih-alih GuardDuty undangan, untuk mengelola akun anggota Anda. Untuk informasi selengkapnya, lihat Mengelola akun dengan AWS Organizations.

Akun yang sudah dikelola oleh akun GuardDuty administrator yang didelegasikan, atau akun anggota aktif yang dikaitkan dengan akun administrator yang didelegasikan tidak dapat ditambahkan ke akun GuardDuty administrator yang didelegasikan lainnya GuardDuty . Setiap organisasi hanya dapat memiliki satu akun GuardDuty administrator yang didelegasikan per Wilayah, dan setiap akun anggota hanya dapat memiliki satu akun GuardDuty administrator yang didelegasikan.

Pilih metode akses yang disukai untuk mengkonsolidasikan akun GuardDuty administrator di bawah satu akun GuardDuty administrator yang didelegasikan.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Untuk masuk, gunakan kredensil akun manajemen organisasi.

2. Semua akun yang ingin Anda kelola GuardDuty harus menjadi bagian dari organisasi Anda. Untuk informasi tentang menambahkan akun ke organisasi Anda, lihat Mengundang Akun AWS untuk bergabung dengan organisasi Anda.
3. Pastikan semua akun anggota dikaitkan dengan akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator tunggal yang didelegasikan. Putuskan hubungan akun anggota yang masih terkait dengan akun administrator yang sudah ada sebelumnya.

   Langkah-langkah berikut akan membantu Anda memisahkan akun anggota dari akun administrator yang sudah ada sebelumnya:

   a. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
   b. Untuk masuk, gunakan kredensil akun administrator yang sudah ada sebelumnya.
   c. Di panel navigasi, pilih Akun.
   d. Pada halaman Akun, pilih satu atau beberapa akun yang ingin Anda pisahkan dari akun administrator.
   e. Pilih Actions dan kemudian pilih Disassociate account.
   f. Pilih Konfirmasi untuk menyelesaikan langkah.
4. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   Untuk masuk, gunakan kredensil akun manajemen.
5. Pada panel navigasi, silakan pilih Pengaturan. Pada halaman Pengaturan, tentukan akun GuardDuty administrator yang didelegasikan untuk organisasi.
6. Masuk ke akun GuardDuty administrator yang didelegasikan yang ditunjuk.
7. Tambahkan anggota dari organisasi. Untuk informasi selengkapnya, lihat Mengelola GuardDuty akun dengan AWS Organizations.

API/CLI

1. Semua akun yang ingin Anda kelola GuardDuty harus menjadi bagian dari organisasi Anda. Untuk informasi tentang menambahkan akun ke organisasi Anda, lihat Mengundang Akun AWS untuk bergabung dengan organisasi Anda.
2. Pastikan semua akun anggota dikaitkan dengan akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator tunggal yang didelegasikan.

   a. Jalankan DisassociateMembersuntuk memisahkan akun anggota yang masih terkait dengan akun administrator yang sudah ada sebelumnya.

b. Atau, Anda dapat menggunakan AWS Command Line Interface untuk menjalankan perintah berikut dan mengganti *777777777777* dengan ID detektor dari akun administrator yang sudah ada sebelumnya dari mana Anda ingin memisahkan akun anggota. Ganti *666666666666* dengan Akun AWS ID akun anggota yang ingin Anda pisahkan.

```
aws guardduty disassociate-members --detector-id 777777777777 --account-
ids 666666666666
```

3. Jalankan EnableOrganizationAdminAccountuntuk mendelegasikan akun GuardDuty administrator Akun AWS sebagai delegasi.

   Atau, Anda dapat menggunakan AWS Command Line Interface untuk menjalankan perintah berikut untuk mendelegasikan akun GuardDuty administrator yang didelegasikan:

```
aws guardduty enable-organization-admin-account --admin-account-id 777777777777
```

4. Tambahkan anggota dari organisasi. Untuk informasi selengkapnya, lihat Create or add member member accounts using API.

> **Important**
>
> Untuk memaksimalkan efektivitas GuardDuty, layanan regional, kami sarankan Anda menunjuk akun GuardDuty administrator yang didelegasikan dan menambahkan semua akun anggota Anda di setiap Wilayah.

GuardDuty pertimbangan untuk mengekspor detail akun anggota dalam format CSV

Sebagai akun GuardDuty administrator, Anda dapat mengekspor detail akun anggota dalam format CSV. Rincian ini mencakup ID akun anggota, nama, jenis (ditambahkan oleh AWS Organizations atau melalui undangan), dan status konfigurasi GuardDuty dan rencana perlindungan khusus.

Opsi Ekspor CSV ditampilkan di halaman GuardDuty Akun berdasarkan cara Anda mengelola beberapa akun anggota. Dengan menggunakan opsi Ekspor CSV, Anda dapat mengidentifikasi akun anggota mana yang mengaktifkan paket perlindungan tertentu.

Daftar berikut memberikan kriteria apakah CSV Ekspor akan tersedia di halaman GuardDuty Akun Anda atau tidak:

- Anda hanya menggunakan AWS Organizations untuk mengelola beberapa akun anggota dan jumlah total akun anggota di GuardDuty organisasi Anda hingga 5.000.
- Anda menggunakan metode keduanya AWS Organizations dan undangan, dan jumlah total akun anggota di GuardDuty organisasi Anda hingga 5.000.

  Dalam skenario ini, CSV yang diekspor akan mencakup apakah akun anggota ditambahkan melalui AWS Organizations atau dengan menggunakan metode berbasis undangan.
- Jika Anda hanya menggunakan metode berbasis undangan untuk mengelola beberapa akun anggota, tidak ada opsi Ekspor CSV.

GuardDuty menemukan jenis

Temuan adalah pemberitahuan yang GuardDuty dihasilkan ketika mendeteksi indikasi aktivitas mencurigakan atau berbahaya di Anda. Akun AWS GuardDuty menghasilkan temuan di akun yang telah diaktifkan GuardDuty.

Untuk informasi tentang perubahan penting pada jenis GuardDuty temuan, termasuk jenis temuan yang baru ditambahkan atau yang sudah pensiun, lihatRiwayat dokumen untuk Amazon GuardDuty.

Untuk informasi tentang menemukan jenis yang sekarang sudah pensiun, lihatTipe temuan yang sudah dihentikan.

GuardDuty Jenis temuan EC2

Temuan berikut ini khusus untuk sumber daya Amazon EC2 dan selalu memiliki Tipe Sumber Daya `Instance`. Tingkat kepelikan dan detail temuan berbeda berdasarkan Peran Sumber Daya, yang menunjukkan apakah sumber daya EC2 adalah target aktivitas mencurigakan atau aktor yang melakukan aktivitas tersebut.

Temuan yang tercantum di sini termasuk sumber data dan model yang digunakan untuk menghasilkan tipe temuan. Untuk informasi selengkapnya tentang sumber data dan model, lihat GuardDuty sumber data dasar.

> **Catatan**
>
> - Detail instans pencarian EC2 mungkin hilang jika instance sudah dihentikan, atau jika panggilan API yang mendasarinya berasal dari instans EC2 di Wilayah lain.
> - Temuan EC2 yang menggunakan log aliran VPC sebagai sumber data tidak mendukung lalu lintas IPv6.

Untuk semua temuan EC2, disarankan untuk memeriksa sumber daya yang bersangkutan untuk menentukan apakah sumber daya tersebut berperilaku seperti dengan yang diharapkan. Jika aktivitas diotorisasi, Anda dapat menggunakan Aturan Penekanan atau daftar IP Tepercaya untuk mencegah notifikasi positif palsu untuk sumber daya tersebut. Jika aktivitas tidak terduga, praktik keamanan terbaik adalah menganggap instans telah disusupi dan mengambil tindakan seperti yang diuraikan dalam Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Topik

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:EC2/UnusualDNSResolver
- DefenseEvasion:EC2/UnusualDoHActivity
- DefenseEvasion:EC2/UnusualDoTActivity
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Custom
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce
- Recon:EC2/PortProbeEMRUnprotectedPort
- Recon:EC2/PortProbeUnprotectedPort
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B

- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/MetadataDNSRebind
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay

Backdoor:EC2/C&CActivity.B

Instans EC2 menanyakan IP yang terkait dengan server perintah dan kontrol yang dikenal.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans yang tercantum dalam lingkungan AWS Anda menanyakan IP yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. Instans yang tercantum mungkin disusupi. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin termasuk PC, server, perangkat seluler, dan perangkat Internet untuk Segala, yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disusupi, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet tersebut, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan Penolakan Layanan Terdistribusi (DDoS).

> **Note**
>
> Jika IP yang ditanyakan terkait log4j, maka bidang temuan terkait akan mencakup nilai-nilai berikut:
>
> - service.additional = Amazon Info.threatListName
> - service.additional Info.threatName = Log4j Terkait

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Backdoor:EC2/C&CActivity.B!DNS

Instans EC2 mengkueri nama domain yang terkait dengan server perintah dan kontrol yang dikenal.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans yang tercantum dalam lingkungan AWS Anda menanyakan nama domain yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. Instans yang tercantum mungkin disusupi. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin termasuk PC, server, perangkat seluler, dan perangkat Internet untuk Segala, yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disusupi, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet tersebut, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan Penolakan Layanan Terdistribusi (DDoS).

> **Note**
>
> Jika nama domain yang dikueri terkait dengan log4j, bidang temuan terkait akan berisi nilai berikut:

- service.additional = Amazon Info.threatListName
- service.additional Info.threatName = Log4j Terkait

> **Note**
>
> Untuk menguji bagaimana GuardDuty menghasilkan jenis temuan ini, Anda dapat membuat permintaan DNS dari instance Anda (menggunakan `dig` untuk Linux atau `nslookup` untuk Windows) terhadap domain `guarddutyc2activityb.com` pengujian.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Backdoor:EC2/DenialOfService.Dns

Instans EC2 berperilaku dengan cara yang mungkin menunjukkan bahwa sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol DNS.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda menghasilkan lalu lintas DNS keluar dalam volume yang besar. Hal ini mungkin menunjukkan bahwa instans yang terdaftar disusupi dan sedang digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol DNS.

> **Note**
>
> Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Backdoor:EC2/DenialOfService.Tcp

Instans EC2 berperilaku dengan cara yang menunjukkan bahwa sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol TCP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda menghasilkan lalu lintas TCP keluar dalam volume yang besar. Hal ini mungkin menunjukkan bahwa instans disusupi dan sedang digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol TCP.

> **Note**
>
> Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Backdoor:EC2/DenialOfService.Udp

Instans EC2 berperilaku dengan cara yang menunjukkan bahwa sedang digunakan untuk melakukan serangan Penolakan Layanan (DoS) menggunakan protokol UDP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yan terdaftar dalam lingkungan AWS Anda menghasilkan lalu lintas UDP keluar dalam volume yang besar. Hal ini mungkin menunjukkan bahwa instans yang terdaftar disusupi dan sedang digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol UDP.

> **Note**
>
> Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Instans EC2 berperilaku dengan cara yang mungkin menunjukkan bahwa sedang digunakan untuk melakukan serangan Penolakan Layanan (DoS) menggunakan protokol UDP pada port TCP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda menghasilkan lalu lintas UDP keluar dalam volume yang besar yang ditargetkan ke port yang biasanya digunakan untuk komunikasi TCP. Hal ini mungkin menunjukkan bahwa instans yang terdaftar disusupi dan sedang digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol UDP pada port TCP.

> **Note**
>
> Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Backdoor:EC2/DenialOfService.UnusualProtocol

Instans EC2 berperilaku dengan cara yang mungkin menunjukkan bahwa sedang digunakan untuk melakukan serangan Penolakan Layanan (DoS) menggunakan protokol yang tidak biasa.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar di lingkungan AWS Anda menghasilkan lalu lintas keluar dalam volume yang besar dari tipe protokol yang tidak biasa yang tidak biasanya digunakan oleh instans EC2, seperti Protokol Manajemen Grup Internet. Hal ini mungkin menunjukkan bahwa instans disusupi dan sedang digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol yang tidak biasa. Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Backdoor:EC2/Spambot

Instans EC2 menunjukkan perilaku yang tidak biasa karena berkomunikasi dengan host jarak jauh pada port 25.

Tingkat keparahan default: Medium

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda berkomunikasi dengan host jarak jauh pada port 25. Perilaku ini tidak biasa karena instans EC2 ini tidak memiliki riwayat komunikasi sebelumnya pada port 25. Port 25 umumnya digunakan oleh server

e-mail untuk komunikasi SMTP. Temuan ini menunjukkan bahwa instans EC2 Anda mungkin disusupi dan digunakan untuk mengirimkan spam.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Behavior:EC2/NetworkPortUnusual

Instans EC2 berkomunikasi dengan host jarak jauh pada port server yang tidak biasa.

Tingkat keparahan default: Medium

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda berperilaku dengan cara yang menyimpang dari garis dasar yang ditetapkan. Instans EC2 ini tidak memiliki riwayat komunikasi pada port jarak jauh ini.

> **Note**
>
> Jika instans EC2 dikomunikasikan pada port 389 atau port 1389, maka tingkat keparahan temuan terkait akan dimodifikasi menjadi Tinggi, dan bidang temuan akan mencakup nilai berikut:
>
> - service.additional Info.context = Kemungkinan log4j callback

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Behavior:EC2/TrafficVolumeUnusual

Instans EC2 menghasilkan lalu lintas jaringan dalam jumlah besar yang tidak biasa ke host jarak jauh.

Tingkat keparahan default: Medium

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda berperilaku dengan cara yang menyimpang dari garis dasar yang ditetapkan. Instans EC2 ini tidak memiliki riwayat pengiriman lalu lintas sebanyak ini ke host jarak jauh ini sebelumnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

CryptoCurrency:EC2/BitcoinTool.B

Instans EC2 mengkueri alamat IP yang terkait dengan aktivitas mata uang kripto.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 yang terdaftar di AWS lingkungan Anda menanyakan Alamat IP yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Bitcoin adalah mata uang kripto dan sistem pembayaran digital yang berlaku di seluruh dunia dan dapat ditukar dengan mata uang, produk, dan layanan lainnya. Bitcoin adalah hasil dari pertambangan bitcoin dan sangat dicari oleh pelaku ancaman.

Rekomendasi remediasi:

Jika Anda menggunakan instans EC2 ini untuk menambang atau mengelola mata uang kripto, atau jika instans ini terlibat dalam aktivitas blockchain, temuan ini bisa jadi aktivitas yang diharapkan untuk lingkungan Anda. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan Anda untuk menetapkan aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atibut Tipe temuan dengan nilai `CryptoCurrency:EC2/BitcoinTool.B`. Kriteria filter kedua harus menggunakan ID Instans dari instans yang terlibat dalam aktivitas blockchain. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat Aturan penindasan di GuardDuty.

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

CryptoCurrency:EC2/BitcoinTool.B!DNS

Instans EC2 menanyakan nama domain yang terkait dengan aktivitas mata uang kripto.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa instans EC2 yang tercantum di lingkungan AWS Anda adalah mengkueri nama domain yang terkait dengan Bitcoin atau aktivitas terkait mata uang kripto lainnya. Bitcoin adalah mata uang kripto dan sistem pembayaran digital yang berlaku di seluruh dunia dan dapat ditukar dengan mata uang, produk, dan layanan lainnya. Bitcoin adalah hasil dari pertambangan bitcoin dan sangat dicari oleh pelaku ancaman.

Rekomendasi remediasi:

Jika Anda menggunakan instans EC2 ini untuk menambang atau mengelola mata uang kripto, atau jika instans ini terlibat dalam aktivitas blockchain, temuan ini bisa jadi aktivitas yang diharapkan untuk lingkungan Anda. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan Anda untuk menetapkan aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atibut Tipe temuan dengan nilai `CryptoCurrency:EC2/BitcoinTool.B!DNS`. Kriteria filter kedua harus menggunakan ID Instans dari instans yang terlibat dalam aktivitas blockchain. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat Aturan penindasan di GuardDuty.

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

DefenseEvasion:EC2/UnusualDNSResolver

Instans Amazon EC2 berkomunikasi dengan resolver DNS publik yang tidak biasa.

Tingkat keparahan default: Medium

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans Amazon EC2 yang tercantum di lingkungan AWS Anda berperilaku dengan cara yang menyimpang dari perilaku acuan dasar. Instans EC2 ini tidak

memiliki riwayat terbaru yang menunjukkan adanya komunikasi dengan resolver DNS publik ini. Bidang yang tidak biasa di panel detail pencarian di GuardDuty konsol dapat memberikan informasi tentang penyelesai DNS yang ditanyakan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

DefenseEvasion:EC2/UnusualDoHActivity

Instans Amazon EC2 melakukan komunikasi DNS melalui HTTPS (DoH) yang tidak biasa.

Tingkat keparahan default: Medium

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans Amazon EC2 yang tercantum di lingkungan AWS Anda berperilaku dengan cara yang menyimpang dari acuan dasar yang ditetapkan. Instans EC2 ini tidak memiliki riwayat terbaru yang menunjukkan adanya komunikasi DNS melalui HTTPS (DoH) dengan server DoH publik ini. Bidang Tidak biasa dalam detail temuan dapat memberikan informasi tentang server DoH yang dimaksud.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

DefenseEvasion:EC2/UnusualDoTActivity

Instans Amazon EC2 melakukan komunikasi DNS melalui TLS (DoT) yang tidak biasa.

Tingkat keparahan default: Medium

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda berperilaku dengan cara yang menyimpang dari garis dasar yang ditetapkan. Instans EC2 ini tidak

memiliki riwayat terbaru yang menunjukkan adanya komunikasi DNS melalui TLS (DoT) dengan server DoT publik ini. Bidang Tidak biasa di panel detail temuan dapat memberikan informasi tentang server DoT yang dimaksud.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Impact:EC2/AbusedDomainRequest.Reputation

Instans EC2 mengkueri nama domain bereputasi rendah yang terkait dengan domain yang diketahui disalahgunakan.

Tingkat keparahan default: Medium

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans Amazon EC2 dalam lingkungan AWS Anda menanyakan nama domain bereputasi rendah yang terkait dengan domain atau alamat IP yang diketahui disalahgunakan. Contoh domain yang disalahgunakan adalah nama domain tingkat atas (TLD) dan nama domain tingkat kedua (2LD) yang menyediakan pendaftaran subdomain gratis serta penyedia DNS dinamis. Pelaku ancaman cenderung menggunakan layanan ini untuk mendaftarkan domain secara gratis atau dengan biaya rendah. Domain bereputasi rendah dalam kategori ini mungkin juga merupakan domain kedaluwarsa yang mencari alamat IP parkir registrar dan oleh karena itu mungkin tidak lagi aktif. IP parkir adalah tempat registrar mengarahkan lalu lintas untuk domain yang belum ditautkan ke layanan apa pun. Instans Amazon EC2 yang tercantum dapat disusupi karena pelaku ancaman biasanya menggunakan layanan registrar ini atau layanan untuk distribusi C&C dan malware.

Domain bereputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberikan peringkat untuk karakteristik domain guna menentukan kemungkinan bahwa domain tersebut berbahaya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Impact:EC2/BitcoinDomainRequest.Reputation

Sebuah instans EC2 sedang mengkueri nama domain dengan reputasi rendah yang terkait dengan aktivitas yang berhubungan dengan mata uang kripto.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa instans Amazon EC2 yang tercantum dalam lingkungan AWS Anda mengkueri nama domain bereputasi rendah yang terkait dengan Bitcoin atau aktivitas mata uang kripto lainnya. Bitcoin adalah mata uang kripto dan sistem pembayaran digital yang berlaku di seluruh dunia dan dapat ditukar dengan mata uang, produk, dan layanan lainnya. Bitcoin adalah hasil dari pertambangan bitcoin dan sangat dicari oleh pelaku ancaman.

Domain bereputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberikan peringkat untuk karakteristik domain guna menentukan kemungkinan bahwa domain tersebut berbahaya.

Rekomendasi remediasi:

Jika Anda menggunakan instans EC2 ini untuk menambang atau mengelola mata uang kripto, atau jika instans ini terlibat dalam aktivitas blockchain, temuan ini dapat merepresentasikan aktivitas yang diharapkan untuk lingkungan Anda. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan Anda untuk menetapkan aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atibut Tipe temuan dengan nilai `Impact:EC2/BitcoinDomainRequest.Reputation`. Kriteria filter kedua harus menggunakan ID Instans dari instans yang terlibat dalam aktivitas blockchain. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat Aturan penindasan di GuardDuty.

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Impact:EC2/MaliciousDomainRequest.Reputation

Instans EC2 menanyakan domain bereputasi rendah yang terkait dengan domain berbahaya yang dikenal.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans Amazon EC2 yang terdaftar dalam lingkungan AWS Anda menanyakan nama domain bereputasi rendah yang terkait dengan domain berbahaya atau alamat IP yang dikenal. Misalnya, domain dapat dikaitkan dengan alamat IP sinkhole yang dikenal. Domain sinkhole adalah domain yang sebelumnya dikendalikan oleh pelaku ancaman, dan permintaan yang dibuat untuk domain tersebut dapat menunjukkan bahwa instans disusupi. Domain ini juga dapat dikorelasikan dengan kampanye berbahaya atau algoritma pembuatan domain yang diketahui.

Domain bereputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberikan peringkat untuk karakteristik domain guna menentukan kemungkinan bahwa domain tersebut berbahaya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Impact:EC2/MaliciousDomainRequest.Custom

Instance EC2 menanyakan domain pada daftar entitas ancaman khusus.

Tingkat keparahan default: Medium

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa instans Amazon EC2 yang terdaftar di lingkungan AWS Anda sedang menanyakan nama domain yang disertakan dalam daftar entitas ancaman yang Anda unggah dan aktifkan. Dalam GuardDuty, daftar entitas ancaman terdiri dari nama domain berbahaya yang diketahui dan alamat IP. GuardDuty menghasilkan temuan berdasarkan aktivitas yang terkait dengan daftar entitas ancaman yang diunggah. Anda dapat melihat nama daftar entitas ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Impact:EC2/PortSweep

Instans EC2 memeriksa port pada sejumlah besar alamat IP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 yang terdaftar di AWS lingkungan Anda sedang menyelidiki port pada sejumlah besar alamat IP yang dapat dirutekan secara publik. Tipe aktivitas ini biasanya digunakan untuk menemukan host yang rentan untuk dieksploitasi. Di panel detail pencarian di GuardDuty konsol Anda, hanya alamat IP jarak jauh terbaru yang ditampilkan

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Impact:EC2/SuspiciousDomainRequest.Reputation

Instans EC2 mengkueri nama domain bereputasi rendah yang mencurigakan karena usia, atau popularitasnya yang rendah.

Tingkat keparahan default: Rendah

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa instans Amazon EC2 yang tercantum dalam lingkungan AWS Anda mengkueri nama domain bereputasi rendah yang diduga berbahaya. Hal ini melihat karakteristik domain ini yang konsisten dengan domain berbahaya yang diamati sebelumnya, namun, model reputasi kami tidak dapat secara pasti menghubungkannya dengan ancaman yang telah diketahui. Domain ini biasanya baru diamati atau menerima jumlah lalu lintas yang rendah.

Domain bereputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberikan peringkat untuk karakteristik domain guna menentukan kemungkinan bahwa domain tersebut berbahaya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Impact:EC2/WinRMBruteForce

Instans EC2 melakukan serangan brute force Windows Remote Management keluar.

Tingkat keparahan default: Rendah*

> **Note**
>
> Tingkat kepelikan temuan ini rendah jika instans EC2 Anda adalah target dari serangan brute force. Tingkat kepelikan temuan ini tinggi jika instans EC2 Anda adalah aktor yang digunakan untuk melakukan serangan brute force.

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 yang terdaftar di AWS lingkungan Anda melakukan serangan brute force Windows Remote Management (WinRM) yang bertujuan untuk mendapatkan akses ke layanan Windows Remote Management pada sistem. Windows-based

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Recon:EC2/PortProbeEMRUnprotectedPort

Instans EC2 memiliki port EMR yang tidak dilindungi yang sedang diperiksa oleh host berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa port sensitif terkait EMR pada instans EC2 yang terdaftar yang merupakan bagian dari cluster di lingkungan AWS Anda tidak diblokir oleh grup keamanan,

daftar kontrol akses (ACL), atau firewall on-host seperti Linux IPTables. Temuan ini juga menginformasikan bahwa pemindai yang dikenal di Internet secara aktif menyelidiki port ini. Port yang dapat memicu temuan ini, seperti port 8088 (YARN Web UI port), berpotensi digunakan untuk eksekusi kode jarak jauh.

Rekomendasi remediasi:

Anda harus memblokir akses terbuka ke port pada klaster dari internet dan membatasi akses hanya ke alamat IP tertentu yang memerlukan akses ke port ini. Untuk informasi selengkapnya, lihat Grup Keamanan untuk Klaster EMR.

Recon:EC2/PortProbeUnprotectedPort

Instans EC2 memiliki port yang tidak dilindungi yang sedang diperiksa oleh host berbahaya yang dikenal.

Tingkat keparahan default: Rendah*

> **Note**
>
> Tingkat kepelikan default temuan ini Rendah. Namun, jika port yang sedang diselidiki, digunakan oleh Elasticsearch (9200 atau 9300), tingkat keparahan temuannya Tinggi.

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa port pada instans EC2 yang terdaftar dalam lingkungan AWS Anda tidak diblokir oleh grup keamanan, daftar kontrol akses (ACL), atau firewall on-host seperti Linux IPTables, dan pemindai yang dikenal di internet memeriksanya secara aktif.

Jika port tidak terlindungi yang teridentifikasi adalah 22 atau 3389 dan Anda menggunakan port ini agar terhubung ke instans Anda, Anda masih dapat membatasi eksposur dengan mengizinkan akses ke port ini hanya untuk alamat IP dari ruang alamat IP jaringan korporat Anda. Untuk membatasi akses ke port 22 di Linux, lihat Otorisasi Lalu Lintas Masuk untuk Instans Linux Anda. Untuk membatasi akses ke port 3389 pada Windows, lihat Mengotorisasi Lalu Lintas Masuk untuk Instans Windows Anda.

GuardDuty tidak menghasilkan temuan ini untuk port 443 dan 80.

Rekomendasi remediasi:

Mungkin terdapat kasus ketika instans sengaja diekspos, misalnya ketika instans menghosting server web. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atibut Tipe temuan dengan nilai `Recon:EC2/PortProbeUnprotectedPort`. Kriteria filter kedua harus sesuai dengan instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID gambar Instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang menghosting alat ini. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat Aturan penindasan di GuardDuty.

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Recon:EC2/Portscan

Instans EC2 melakukan pemindaian port keluar ke host jarak jauh.

Tingkat keparahan default: Medium

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda kemungkinan terlibat dalam serangan pemindaian port karena mencoba untuk menghubungkan ke beberapa port dalam waktu yang singkat. Tujuan serangan pemindaian port adalah untuk menemukan port terbuka guna menemukan layanan mana yang dijalankan mesin dan untuk mengidentifikasi sistem operasinya.

Rekomendasi remediasi:

Temuan ini bisa menjadi positif palsu ketika aplikasi penilaian kerentanan diterapkan pada instans EC2 di lingkungan Anda karena aplikasi ini melakukan pemindaian port untuk mengingatkan Anda tentang port terbuka yang salah konfigurasi. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atibut Tipe temuan dengan nilai `Recon:EC2/Portscan`. Kriteria filter kedua harus sesuai dengan instans yang menghosting alat penilaian kerentanan ini. Anda dapat menggunakan atribut ID gambar Instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang menghosting alat ini. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat Aturan penindasan di GuardDuty.

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Trojan:EC2/BlackholeTraffic

Instans EC2 mencoba untuk berkomunikasi dengan alamat IP dari host jarak jauh yang dikenal sebagai black hole.

Tingkat keparahan default: Medium

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 yang terdaftar di AWS lingkungan Anda mungkin terganggu karena mencoba berkomunikasi dengan alamat IP lubang hitam (atau lubang wastafel). Black hole adalah tempat di jaringan di mana lalu lintas yang masuk atau keluar diam-diam dibuang tanpa menginformasikan sumber bahwa datanya tidak sampai ke penerima yang dimaksudkan. Alamat IP black hole menentukan mesin host yang tidak berjalan atau alamat yang tidak memiliki host yang ditetapkan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Trojan:EC2/BlackholeTraffic!DNS

Instans EC2 mengkueri nama domain yang sedang diarahkan ke alamat IP black hole.

Tingkat keparahan default: Medium

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa instans EC2 yang terdaftar di AWS lingkungan Anda mungkin terganggu karena menanyakan nama domain yang sedang dialihkan ke alamat IP lubang hitam. Black hole adalah tempat di jaringan di mana lalu lintas yang masuk atau keluar diam-diam dibuang tanpa menginformasikan sumber bahwa datanya tidak sampai ke penerima yang dimaksudkan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Trojan:EC2/DGADomainRequest.B

Instans EC2 menanyakan domain yang dihasilkan dengan algoritme. Domain tersebut umumnya digunakan oleh malware dan dapat menjadi indikasi instans EC2 yang disusupi.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda mencoba menanyakan domain algoritme pembuatan domain (DGA). Instans EC2 Anda mungkin disusupi.

DGAs digunakan untuk secara berkala menghasilkan sejumlah besar nama domain yang dapat digunakan sebagai titik pertemuan dengan server perintah dan kontrol (C&C) mereka. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah kepada anggota botnet, yang merupakan kumpulan perangkat yang terhubung ke internet yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Banyaknya kemungkinan titik pertemuan menyulitkan untuk mematikan botnet secara efektif karena komputer yang terinfeksi berusaha menghubungi beberapa nama domain ini setiap hari untuk menerima pembaruan atau perintah.

> **Note**
>
> Temuan ini didasarkan pada analisis nama domain menggunakan heuristik lanjutan dan dapat mengidentifikasi domain DGA baru yang tidak terdapat dalam umpan intelijen ancaman.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Trojan:EC2/DGADomainRequest.C!DNS

Instans EC2 menanyakan domain yang dihasilkan dengan algoritme. Domain tersebut umumnya digunakan oleh malware dan dapat menjadi indikasi instans EC2 yang disusupi.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda mencoba menanyakan domain algoritme pembuatan domain (DGA). Instans EC2 Anda mungkin disusupi.

DGAs digunakan untuk secara berkala menghasilkan sejumlah besar nama domain yang dapat digunakan sebagai titik pertemuan dengan server perintah dan kontrol (C&C) mereka. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah kepada anggota botnet, yang merupakan kumpulan perangkat yang terhubung ke internet yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Banyaknya kemungkinan titik pertemuan menyulitkan untuk mematikan botnet secara efektif karena komputer yang terinfeksi berusaha menghubungi beberapa nama domain ini setiap hari untuk menerima pembaruan atau perintah.

> **Note**
>
> Temuan ini didasarkan pada domain DGA yang diketahui dari GuardDuty umpan intelijen ancaman.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Trojan:EC2/DNSDataExfiltration

Instans EC2 mengekstraksi data melalui kueri DNS.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda menjalankan malware yang menggunakan kueri DNS untuk transfer data keluar. Tipe transfer data ini merupakan indikasi dari instans yang disusupi dan dapat mengakibatkan eksfiltrasi data. Lalu lintas DNS biasanya tidak diblokir oleh firewall. Misalnya, malware dalam instans EC2 yang disusupi dapat mengkodekan data, (seperti nomor kartu kredit Anda), menjadi kueri DNS dan mengirimkannya ke server DNS jarak jauh yang dikendalikan oleh penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Trojan:EC2/DriveBySourceTraffic!DNS

Instans EC2 menanyakan nama domain dari host jarak jauh yang merupakan sumber serangan Drive-By unduhan yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda mungkin disusupi karena menanyakan nama domain dari host jarak jauh yang merupakan sumber serangan unduhan drive-by yang diketahui. Hal ini merupakan unduhan perangkat lunak komputer yang tidak diinginkan dari internet yang dapat memicu penginstalan virus, spyware, atau malware secara otomatis.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Trojan:EC2/DropPoint

Instans EC2 mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang diketahui menyimpan kredensial dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Medium

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda mencoba berkomunikasi dengan alamat IP host jarak jauh yang diketahui memiliki kredensyal dan data curian lainnya yang ditangkap oleh malware.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Trojan:EC2/DropPoint!DNS

Instans EC2 mengkueri nama domain dari host jarak jauh yang diketahui menyimpan kredensial dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Medium

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda menanyakan nama domain host jarak jauh yang diketahui memiliki kredensyal dan data curian lainnya yang ditangkap oleh malware.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Trojan:EC2/PhishingDomainRequest!DNS

Instans EC2 mengkueri domain yang terlibat dalam serangan phishing. Instans EC2 Anda mungkin disusupi.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa terdapat instans EC2 dalam lingkungan AWS Anda yang mencoba menanyakan domain yang terlibat dalam serangan phishing. Domain phishing dibuat oleh seseorang yang menyamar sebagai institusi yang sah untuk membujuk individu agar memberikan data sensitif, seperti informasi pengenal pribadi, detail kartu kredit dan perbankan, serta kata sandi. Instans EC2 Anda mungkin mencoba mengambil data sensitif yang disimpan di situs web phishing, atau mungkin mencoba membuat situs web phishing. Instans EC2 Anda mungkin disusupi.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Instans EC2 membuat koneksi ke alamat IP pada daftar ancaman kustom.

Tingkat keparahan default: Medium

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda berkomunikasi dengan alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Dalam GuardDuty, daftar ancaman terdiri dari alamat IP berbahaya yang diketahui. GuardDutymenghasilkan temuan berdasarkan daftar ancaman yang diunggah. Daftar ancaman yang digunakan untuk menghasilkan temuan ini akan tercantum dalam detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

UnauthorizedAccess:EC2/MetadataDNSRebind

Instans EC2 melakukan pencarian DNS untuk layanan metadata instans.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda menanyakan domain yang menyelesaikan alamat IP metadata EC2 (169.254.169.254). Kueri DNS semacam ini dapat menunjukkan bahwa instans adalah target dari teknik rebinding DNS. Teknik ini dapat digunakan untuk mendapatkan metadata dari instans EC2, termasuk kredensial IAM yang terkait dengan instans.

Rebinding DNS adalah proses yang menipu sebuah aplikasi yang berjalan di instans EC2 untuk memuat data pengembalian dari URL, dengan nama domain di URL tersebut di-resolve menjadi alamat IP metadata EC2 (169.254.169.254). Hal ini menyebabkan aplikasi mengakses metadata EC2 dan mungkin membuatnya tersedia untuk penyerang.

Metadata EC2 dapat diakses menggunakan rebinding DNS hanya jika instans EC2 menjalankan aplikasi rentan yang memungkinkan injeksi URL, atau jika seseorang mengakses URL di browser web yang berjalan pada instans EC2.

Rekomendasi remediasi:

Menanggapi temuan ini, Anda harus mengevaluasi apakah ada aplikasi rentan yang berjalan pada instans EC2, atau jika seseorang menggunakan browser untuk mengakses domain yang diidentifikasi dalam temuan. Jika akar penyebabnya adalah aplikasi yang rentan, Anda harus memperbaiki kerentanannya. Jika seseorang menjelajahi domain yang diidentifikasi, Anda harus memblokir domain atau mencegah pengguna mengaksesnya. Jika Anda menentukan temuan ini terkait dengan kedua kasus di atas, cabut sesi yang terkait dengan instans EC2.

Beberapa AWS pelanggan sengaja memetakan alamat IP metadata ke nama domain di server DNS otoritatif mereka. Jika hal ini dilakukan di lingkungan Anda, kami menyarankan Anda untuk membuat aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atibut Tipe temuan dengan nilai `UnauthorizedAccess:EC2/MetaDataDNSRebind`. Kriteria filter kedua harus menggunakan Domain permintaan DNS dan nilainya harus sesuai dengan domain yang telah Anda petakan ke alamat IP (169.254.169.254)

metadata. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat Aturan penindasan di GuardDuty.

UnauthorizedAccess:EC2/RDPBruteForce

Instans EC2 telah terlibat dalam serangan brute force RDP.

Tingkat keparahan default: Rendah*

> **Note**
>
> Tingkat kepelikan temuan ini rendah jika instans EC2 Anda adalah target dari serangan brute force. Tingkat kepelikan temuan ini tinggi jika instans EC2 Anda adalah aktor yang digunakan untuk melakukan serangan brute force.

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda terlibat dalam serangan brute force yang bertujuan mendapatkan kata sandi ke layanan RDP pada sistem. Windows-based Hal ini dapat mengindikasikan akses yang tidak sah ke sumber daya AWS Anda.

Rekomendasi remediasi:

Jika Peran Sumber Daya instans Anda adalah `ACTOR`, hal ini mengindikasikan bahwa instans Anda telah digunakan untuk melakukan serangan brute force RDP. Kecuali instans ini memiliki alasan yang sah untuk menghubungi alamat IP yang terdaftar sebagai `Target`, Anda disarankan untuk menganggap bahwa instans Anda telah disusupi dan mengambil tindakan yang tercantum di Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Jika Peran Sumber Daya instans Anda adalah `TARGET`, temuan ini dapat diperbaiki dengan mengamankan port RDP Anda hanya ke IP yang tepercaya melalui Grup Keamanan, ACL, atau firewall. Untuk informasi selengkapnya, lihat Tip untuk mengamankan instans EC2 Anda (Linux).

UnauthorizedAccess:EC2/SSHBruteForce

Instans EC2 telah terlibat dalam serangan brute force SSH.

Tingkat keparahan default: Rendah*

> **Note**
>
> Tingkat kepelikan temuan ini rendah jika serangan brute force ditujukan pada salah satu instans EC2 Anda. Tingkat kepelikan temuan ini tinggi jika instans EC2 Anda sedang digunakan untuk melakukan serangan brute force.

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda terlibat dalam serangan brute force yang bertujuan mendapatkan kata sandi ke layanan SSH pada sistem. Linux-based Hal ini dapat mengindikasikan akses yang tidak sah ke sumber daya AWS Anda.

> **Note**
>
> Temuan ini dihasilkan hanya melalui pemantauan lalu lintas pada port 22. Jika layanan SSH Anda dikonfigurasi untuk menggunakan port lain, temuan ini tidak dihasilkan.

Rekomendasi remediasi:

Jika target upaya brute force adalah host benteng, ini mungkin mewakili perilaku yang diharapkan untuk lingkungan Anda AWS . Jika demikian, kami menyarakan Anda untuk membuat aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atibut Tipe temuan dengan nilai `UnauthorizedAccess:EC2/SSHBruteForce`. Kriteria filter kedua harus sesuai dengan instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID gambar Instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang menghosting alat ini. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat Aturan penindasan di GuardDuty.

Jika aktivitas ini tidak diharapkan untuk lingkungan Anda dan jika Peran Sumber Daya instans Anda adalah `TARGET`, temuan ini dapat diperbaiki dengan mengamankan port SSH Anda hanya ke IP yang tepercaya melalui Grup Keamanan, ACL, atau firewall. Untuk informasi selengkapnya, lihat Tip untuk mengamankan instans EC2 Anda (Linux).

Jika Peran Sumber Daya instans Anda adalah `ACTOR`, hal ini mengindikasikan bahwa instans telah digunakan untuk melakukan serangan brute force SSH. Kecuali instans ini memiliki alasan yang sah untuk menghubungi alamat IP yang terdaftar sebagai `Target`, Anda disarankan untuk menganggap

bahwa instans Anda telah disusupi dan mengambil tindakan yang tercantum di Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

UnauthorizedAccess:EC2/TorClient

Instans EC2 Anda membuat koneksi ke Tor Guard atau node Authority.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda membuat koneksi ke Tor Guard atau node Authority. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Node Tor Guards dan Authority bertindak sebagai gateway awal ke dalam jaringan Tor. Lalu lintas ini dapat mengindikasikan bahwa instans EC2 ini telah disusupi dan bertindak sebagai klien pada jaringan Tor. Temuan ini mungkin menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

UnauthorizedAccess:EC2/TorRelay

Instans EC2 Anda membuat koneksi ke jaringan Tor sebagai relai Tor.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda membuat koneksi ke jaringan Tor dengan cara yang menunjukkan bahwa itu bertindak sebagai relai Tor. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Tor meningkatkan anonimitas komunikasi dengan meneruskan lalu lintas klien yang kemungkinan terlarang dari satu relai Tor ke relai lainnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Lihat informasi yang lebih lengkap di Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

GuardDuty Jenis pencarian IAM

Temuan berikut ini khusus untuk entitas IAM dan access key serta selalu memiliki Tipe Sumber Daya dari `AccessKey`. Tingkat kepelikan dan detail temuan berbeda berdasarkan tipe temuan.

Temuan yang tercantum di sini termasuk sumber data dan model yang digunakan untuk menghasilkan tipe temuan. Untuk informasi selengkapnya, lihat GuardDuty sumber data dasar.

Untuk semua IAM-related temuan, kami menyarankan Anda memeriksa entitas yang bersangkutan dan memastikan bahwa izin mereka mengikuti praktik terbaik dengan hak istimewa paling sedikit. Jika aktivitas tidak terduga, kredensial mungkin disusupi. Untuk informasi tentang remediasi temuan, lihatMemperbaiki potensi terganggu AWS credentials.

Topik

- CredentialAccess:IAMUser/AnomalousBehavior
- CredentialAccess:IAMUser/CompromisedCredentials
- DefenseEvasion:IAMUser/AnomalousBehavior
- DefenseEvasion:IAMUser/BedrockLoggingDisabled
- Discovery:IAMUser/AnomalousBehavior
- Exfiltration:IAMUser/AnomalousBehavior
- Impact:IAMUser/AnomalousBehavior
- InitialAccess:IAMUser/AnomalousBehavior
- PenTest:IAMUser/KaliLinux
- PenTest:IAMUser/ParrotLinux
- PenTest:IAMUser/PentooLinux
- Persistence:IAMUser/AnomalousBehavior
- Policy:IAMUser/RootCredentialUsage
- Policy:IAMUser/ShortTermRootCredentialUsage
- PrivilegeEscalation:IAMUser/AnomalousBehavior
- Recon:IAMUser/MaliciousIPCaller
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled

- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

API yang digunakan untuk mendapatkan akses ke AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa terdapat permintaan API beranomali yang diamati di akun Anda. Temuan ini dapat mencakup satu permintaan API atau serangkaian permintaan API terkait yang dibuat di sekitar oleh satu identitas pengguna. API yang diamati umumnya berkaitan dengan tahap akses kredensial serangan ketika musuh mencoba mengumpulkan kata sandi, nama pengguna, dan access key untuk lingkungan Anda. API dalam kategori ini adalah`GetPasswordData`,`GetSecretValue`,`BatchGetSecretValue`, dan`GenerateDbAuthToken`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa beranomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan API spesifik yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang menginvokasi permintaan dapat ditemukan di detail temuan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

CredentialAccess:IAMUser/CompromisedCredentials

Kunci akses IAM berpotensi disusupi menurut identifikasi intelijen ancaman Amazon.

Tingkat keparahan default: Tinggi

- Fitur: Termasuk dengan Perlindungan Sumber Data Dasar

Deskripsi lengkap:

Temuan ini memberi tahu Anda bahwa kunci akses IAM yang terkait dengan AWS akun Anda telah diidentifikasi berpotensi dikompromikan oleh intelijen ancaman Amazon. Kredensi yang disusupi kemudian digunakan untuk menjalankan operasi API di lingkungan Anda. AWS Daftar panggilan API yang dilakukan menggunakan kredensial yang disusupi, beserta jumlah dan stempel waktu setiap panggilan, kunci akses yang terlibat, dan alamat IP sumber disertakan dalam detail temuan.

Kompromi kredenal dalam temuan ini diidentifikasi oleh intelijen ancaman Amazon. AWS memantau kredensil yang berpotensi dikompromikan melalui pola penggunaan dan menghasilkan temuan ini ketika kredensi seperti itu diamati sedang digunakan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

DefenseEvasion:IAMUser/AnomalousBehavior

API yang digunakan untuk menghindari tindakan defensif diinvokasi dengan cara yang beranomali.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa terdapat permintaan API beranomali yang diamati di akun Anda. Temuan ini mungkin mencakup permintaan satu API atau serangkaian API yang terkait yang dibuat berdekatan oleh satu identitas pengguna. API yang diamati umumnya berkaitan dengan taktik

penghindaran pertahanan ketika penyerang mencoba menutupi jejak mereka agar tidak terdeteksi. API dalam kategori ini biasanya menghapus, menonaktifkan, atau menghentikan operasi, seperti, `DeleteFlowLogs`, `DisableAlarmActions`, atau `StopLogging`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa beranomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan API spesifik yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang menginvokasi permintaan dapat ditemukan di detail temuan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

DefenseEvasion:IAMUser/BedrockLoggingDisabled

Pencatatan log untuk Amazon Bedrock dinonaktifkan.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa pencatatan log dinonaktifkan untuk invokasi model Bedrock di akun Anda. Ini bisa jadi adalah upaya penyerang untuk menyamarkan aktivitas berbahaya seperti eksfiltrasi data atau penyalahgunaan model AI. Ketika pencatatan log dinonaktifkan, tidak akan ada visibilitas tentang data yang dikirim ke model dan bagaimana model digunakan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Discovery:IAMUser/AnomalousBehavior

API yang biasa digunakan untuk menemukan sumber daya diinvokasi dengan cara yang beranomali.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa terdapat permintaan API beranomali yang diamati di akun Anda. Temuan ini mungkin mencakup permintaan satu API atau serangkaian API yang terkait yang dibuat berdekatan oleh satu identitas pengguna. API yang diamati umumnya dikaitkan dengan tahap penemuan serangan ketika musuh mengumpulkan informasi untuk menentukan apakah AWS lingkungan Anda rentan terhadap serangan yang lebih luas. API dalam kategori ini biasanya mendapatkan, mendeskripsikan, atau menampilkan daftar operasi, seperti, `DescribeInstances`, `GetRolePolicy`, atau `ListAccessKeys`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa beranomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan API spesifik yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang menginvokasi permintaan dapat ditemukan di detail temuan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Exfiltration:IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mengumpulkan data dari AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa terdapat permintaan API beranomali yang diamati di akun Anda. Temuan ini mungkin mencakup permintaan satu API atau serangkaian API yang terkait yang dibuat berdekatan oleh satu identitas pengguna. API yang diamati umumnya berkaitan dengan taktik eksfiltrasi ketika penyerang mencoba mengumpulkan data dari jaringan Anda menggunakan pengemasan dan enkripsi agar tidak terdeteksi. API untuk tipe temuan ini hanya merupakan operasi manajemen (bidang kontrol) dan biasanya terkait dengan S3, snapshot, dan basis data, seperti, `PutBucketReplication`, `CreateSnapshot`, atau `RestoreDBInstanceFromDBSnapshot`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa beranomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan API spesifik yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang menginvokasi permintaan dapat ditemukan di detail temuan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Impact:IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mengutak-atik data atau proses dalam AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa terdapat permintaan API beranomali yang diamati di akun Anda. Temuan ini mungkin mencakup permintaan satu API atau serangkaian API yang terkait yang dibuat berdekatan oleh satu identitas pengguna. API yang diamati biasanya berkaitan dengan taktik dampak ketika penyerang mencoba mengganggu operasi dan memanipulasi, mengganggu, atau menghancurkan data di akun Anda. API untuk tipe temuan ini biasanya merupakan operasi operasi hapus, perbarui, atau tempatkan, seperti, `DeleteSecurityGroup`, `UpdateUser`, atau `PutBucketPolicy`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa beranomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan API spesifik yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang menginvokasi permintaan dapat ditemukan di detail temuan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

InitialAccess:IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mendapatkan akses tidak sah ke AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa terdapat permintaan API beranomali yang diamati di akun Anda. Temuan ini mungkin mencakup permintaan satu API atau serangkaian API yang terkait yang dibuat berdekatan oleh satu identitas pengguna. API yang diamati umumnya berkaitan dengan tahap akses awal serangan ketika penyerang mencoba memperoleh akses ke lingkungan Anda. API dalam kategori ini biasanya mendapatkan token, atau operasi sesi, seperti,`StartSession`, atau`GetAuthorizationToken`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa beranomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan API spesifik yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang menginvokasi permintaan dapat ditemukan di detail temuan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

PenTest:IAMUser/KaliLinux

API dipanggil dari mesin Kali Linux.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Kali Linux melakukan panggilan API menggunakan kredensil milik AWS akun yang terdaftar di lingkungan Anda. Kali Linux adalah alat uji penetrasi populer yang digunakan oleh para profesional keamanan untuk mengidentifikasi

kelemahan dalam instans EC2 yang memerlukan patch. Penyerang juga menggunakan alat ini untuk menemukan kelemahan konfigurasi EC2 dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

PenTest:IAMUser/ParrotLinux

API diinvokasi dari mesin Parrot Security Linux.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Parrot Security Linux melakukan panggilan API menggunakan kredensil milik AWS akun yang terdaftar di lingkungan Anda. Parrot Security Linux adalah alat uji penetrasi populer yang digunakan oleh para profesional keamanan untuk mengidentifikasi kelemahan dalam instans EC2 yang memerlukan patch. Penyerang juga menggunakan alat ini untuk menemukan kelemahan konfigurasi EC2 dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

PenTest:IAMUser/PentooLinux

API diinvokasi dari mesin Pentoo Linux.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Pentoo Linux melakukan panggilan API menggunakan kredensil milik AWS akun yang terdaftar di lingkungan Anda. Pentoo Linux adalah

alat uji penetrasi populer yang digunakan oleh para profesional keamanan untuk mengidentifikasi kelemahan dalam instans EC2 yang memerlukan patch. Penyerang juga menggunakan alat ini untuk menemukan kelemahan konfigurasi EC2 dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Persistence:IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mempertahankan akses tidak sah ke AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa terdapat permintaan API beranomali yang diamati di akun Anda. Temuan ini mungkin mencakup permintaan satu API atau serangkaian API yang terkait yang dibuat berdekatan oleh satu identitas pengguna. API yang diamati umumnya berkaitan dengan taktik persistensi ketika penyerang telah memperoleh akses ke lingkungan Anda dan mencoba mempertahankan akses tersebut. API dalam kategori ini biasanya membuat, mengimpor, atau memodifikasi operasi, seperti, `CreateAccessKey`, `ImportKeyPair`, atau `ModifyInstanceAttribute`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa beranomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan API spesifik yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang menginvokasi permintaan dapat ditemukan di detail temuan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Policy:IAMUser/RootCredentialUsage

API dipanggil menggunakan kredenal masuk pengguna root.

Tingkat keparahan default: Rendah

- Sumber data: peristiwa CloudTrail manajemen atau peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa kredenal masuk pengguna root dari yang tercantum Akun AWS di lingkungan Anda digunakan untuk membuat permintaan ke layanan. AWS Disarankan agar pengguna tidak pernah menggunakan kredenal masuk pengguna root untuk mengakses layanan. AWS Sebagai gantinya, AWS layanan harus diakses menggunakan kredensi sementara hak istimewa terkecil dari AWS Security Token Service (STS). Jika AWS STS tidak didukung, sebaiknya gunakan kredensial pengguna IAM. Untuk informasi lebih lanjut, lihat Praktik Terbaik IAM.

> **Note**
>
> Jika Perlindungan S3 diaktifkan untuk akun, maka temuan ini dapat dihasilkan sebagai tanggapan atas upaya untuk menjalankan operasi bidang data S3 di sumber daya Amazon S3 dengan menggunakan kredenal masuk pengguna root dari file. Akun AWS Panggilan API yang digunakan akan tercantum dalam detail temuan. Jika Perlindungan S3 tidak diaktifkan, maka temuan ini hanya dapat dipicu oleh API log Peristiwa. Untuk informasi lebih lanjut tentang Perlindungan S3, lihatPerlindungan S3.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Policy:IAMUser/ShortTermRootCredentialUsage

API diinvokasi menggunakan kredensial pengguna root yang dibatasi.

Tingkat keparahan default: Rendah

- Sumber data: peristiwa AWS CloudTrail manajemen atau peristiwa AWS CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa kredensi pengguna terbatas yang dibuat untuk yang terdaftar Akun AWS di lingkungan Anda, sedang digunakan untuk membuat permintaan. Layanan AWS Disarankan untuk menggunakan kredensi pengguna root hanya untuk tugas-tugas yang memerlukan kredensi pengguna root.

Jika memungkinkan, akses peran IAM Layanan AWS dengan menggunakan hak istimewa terkecil dengan kredensi sementara dari (). AWS Security Token Service AWS STS Untuk skenario di AWS STS mana tidak didukung, praktik terbaik adalah menggunakan kredensional pengguna IAM. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan dalam praktik terbaik pengguna IAM dan Root untuk Anda Akun AWS di Panduan Pengguna IAM.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

PrivilegeEscalation:IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mendapatkan izin tingkat tinggi AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa terdapat permintaan API beranomali yang diamati di akun Anda. Temuan ini mungkin mencakup permintaan satu API atau serangkaian API yang terkait yang dibuat berdekatan oleh satu identitas pengguna. API yang diamati umumnya terkait dengan taktik eskalasi hak akses saat penyerang mencoba mendapatkan tingkat izin yang lebih tinggi untuk sebuah lingkungan. API dalam kategori ini biasanya melibatkan operasi yang mengubah kebijakan, peran, dan pengguna IAM, seperti, `AssociateIamInstanceProfile`, `AddUserToGroup`, atau `PutUserPolicy`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa beranomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan API spesifik yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang menginvokasi permintaan dapat ditemukan di detail temuan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Recon:IAMUser/MaliciousIPCaller

API diinvokasi dari alamat IP berbahaya yang sudah diketahui.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa operasi API yang dapat menampilkan daftar atau mendeskripsikan sumber daya AWS di akun dalam lingkungan Anda diinvokasi dari alamat IP yang termasuk dalam daftar ancaman. Penyerang dapat menggunakan kredensil curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensil yang lebih berharga atau menentukan kemampuan kredensil yang sudah mereka miliki.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Recon:IAMUser/MaliciousIPCaller.Custom

API diinvokasi dari alamat IP berbahaya yang sudah diketahui.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa operasi API yang dapat menampilkan daftar atau mendeskripsikan sumber daya AWS di akun dalam lingkungan Anda diinvokasi dari alamat IP yang termasuk dalam daftar ancaman kustom. Daftar ancaman yang digunakan akan dicantumkan dalam detail temuan. Seorang penyerang mungkin menggunakan kredensil curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensil yang lebih berharga atau menentukan kemampuan kredensil yang sudah mereka miliki.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Recon:IAMUser/TorIPCaller

API diinvokasi dari alamat IP simpul keluar Tor.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa operasi API yang dapat menampilkan daftar atau mendeskripsikan sumber daya AWS di akun dalam lingkungan anda diinvokasi dari alamat IP simpul keluar Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Node Tor terakhir disebut sebagai nod keluar. Penyerang akan menggunakan Tor untuk menutupi identitas mereka yang sebenarnya.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail logging dinonaktifkan.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa CloudTrail jejak di AWS lingkungan Anda dinonaktifkan. Hal ini bisa menjadi percobaan penyerang untuk menonaktifkan pencatatan log untuk menutupi jejak mereka dengan menghilangkan jejak aktivitas mereka sekaligus mendapatkan akses ke sumber daya AWS Anda untuk tujuan berbahaya. Temuan ini dapat dipicu oleh penghapusan sukses atau pembaruan jejak. Temuan ini juga dapat dipicu oleh penghapusan bucket S3 yang berhasil menyimpan log dari jejak yang terkait dengannya. GuardDuty

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Stealth:IAMUser/PasswordPolicyChange

Kebijakan kata sandi akun dilemahkan.

Tingkat keparahan default: Rendah*

> **Note**
>
> Tingkat keparahan temuan ini bisa Rendah, Sedang, atau Tinggi tergantung pada tingkat keparahan perubahan yang dibuat pada kebijakan kata sandi.

- Sumber data: acara CloudTrail manajemen

Kebijakan kata sandi AWS akun dilemahkan pada akun yang terdaftar di AWS lingkungan Anda. Misalnya, kebijakan ini dihapus atau diubah sehingga membutuhkan karakter yang lebih sedikit, tidak mewajibkan simbol dan angka, atau memperpanjang masa kedaluwarsa kata sandi. Temuan ini juga dapat dipicu oleh upaya untuk memperbarui atau menghapus kebijakan kata sandi AWS akun Anda. Kebijakan kata sandi AWS akun mendefinisikan aturan yang mengatur jenis kata sandi apa yang dapat ditetapkan untuk pengguna IAM Anda. Kebijakan kata sandi yang lebih lemah memungkinkan pembuatan kata sandi yang mudah diingat dan berpotensi lebih mudah ditebak, sehingga menciptakan risiko keamanan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Terdeteksi sejumlah login konsol yang berhasil di seluruh dunia.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa beberapa login konsol yang berhasil untuk pengguna IAM yang sama diamati pada waktu yang sama di berbagai lokasi geografis. Pola lokasi akses anomali dan berisiko seperti itu menunjukkan potensi akses tidak sah ke sumber daya Anda. AWS

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Kredensial yang dibuat secara eksklusif untuk instans EC2 melalui peran peluncuran Instans digunakan dari akun lain di dalamnya AWS.

Tingkat keparahan default: Tinggi*

> **Note**
>
> Tingkat keparahan default temuan ini adalah Tinggi. Namun, jika API dipanggil oleh akun yang berafiliasi dengan AWS lingkungan Anda, tingkat keparahannya adalah Medium.

- Sumber data: peristiwa CloudTrail manajemen atau peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda kapan kredenal instans Amazon EC2 Anda digunakan untuk memanggil API dari alamat IP atau titik akhir VPC Amazon, yang dimiliki oleh akun yang AWS berbeda dari akun yang dijalankan instans Amazon EC2 terkait. Deteksi titik akhir VPC hanya tersedia untuk layanan yang mendukung peristiwa aktivitas jaringan untuk titik akhir VPC. Untuk informasi tentang layanan yang mendukung peristiwa aktivitas jaringan untuk titik akhir VPC, lihat Mencatat log peristiwa aktivitas jaringan di Panduan Pengguna AWS CloudTrail .

AWS tidak merekomendasikan untuk mendistribusikan ulang kredensi sementara di luar entitas yang membuatnya (misalnya, aplikasi, AWS Amazon EC2, atau). AWS Lambda Namun, pengguna yang berwenang dapat mengekspor kredensial dari instans Amazon EC2 mereka untuk membuat panggilan API yang sah. Jika `remoteAccountDetails.Affiliated` bidangnya adalah `True` API dipanggil dari akun yang terkait dengan akun administrator yang sama. Untuk mengesampingkan potensi serangan dan memverifikasi legitimasi aktivitas, hubungi Akun AWS pemilik atau kepala IAM kepada siapa kredensi ini diberikan.

> **Note**
>
> Jika GuardDuty mengamati aktivitas lanjutan dari akun jarak jauh, model pembelajaran mesin (ML) akan mengidentifikasi ini sebagai perilaku yang diharapkan. Oleh karena itu, GuardDuty akan berhenti menghasilkan temuan ini untuk aktivitas dari akun jarak jauh itu. GuardDuty akan terus menghasilkan temuan untuk perilaku baru dari akun jarak jauh lainnya dan akan mengevaluasi kembali akun jarak jauh yang dipelajari saat perilaku berubah seiring waktu.

Rekomendasi perbaikan:

Temuan ini akan dihasilkan saat permintaan AWS API dibuat di dalam AWS melalui instans Amazon EC2 di luar instans Anda Akun AWS, dengan menggunakan kredenal sesi instans Amazon EC2 Anda. Mungkin lazim, seperti untuk arsitektur Transit Gateway dalam konfigurasi hub dan spoke, untuk merutekan lalu lintas melalui AWS VPC jalan keluar hub tunggal dengan titik akhir layanan. Jika perilaku ini diharapkan, maka GuardDuty sarankan Anda untuk menggunakan Aturan penekanan dan membuat aturan dengan kriteria dua filter. Kriteria pertama adalah tipe temuan, yang dalam hal ini adalah UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS. Kriteria filter kedua adalah ID akun jarak jauh pada detail akun jarak jauh.

Untuk menanggapi temuan ini, Anda dapat menggunakan alur kerja berikut untuk menentukan tindakan:

1. Identifikasi akun jarak jauh yang terlibat dari bidang `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Tentukan apakah akun itu berafiliasi dengan GuardDuty lingkungan Anda dari `service.action.awsApiCallAction.remoteAccountDetails.affiliated` lapangan.
3. Jika akun tersebut berafiliasi, hubungi pemilik akun jarak jauh serta pemilik kredensial instans Amazon EC2 dan minta mereka menyelidikinya.

   Jika akun tidak berafiliasi, maka langkah pertama adalah mengevaluasi apakah akun tersebut terkait dengan organisasi Anda tetapi bukan bagian dari pengaturan lingkungan beberapa GuardDuty akun Anda, atau jika GuardDuty belum diaktifkan di akun ini. Selanjutnya, hubungi pemilik kredensial instans Amazon EC2 untuk menentukan apakah terdapat kasus penggunaan akun jarak jauh yang menggunakan kredensial ini.
4. Jika pemilik kredensial tidak mengenali akun jarak jauh tersebut, kredensial mungkin telah disusupi oleh pelaku ancaman yang beroperasi di dalam AWS. Anda harus mengambil langkah-langkah

yang direkomendasikanMemperbaiki instans Amazon EC2 yang berpotensi dikompromikan, untuk mengamankan lingkungan Anda.

Selain itu, Anda dapat mengirimkan laporan penyalahgunaan ke tim AWS Trust and Safety untuk memulai penyelidikan ke akun jarak jauh. Saat mengirimkan laporan Anda ke AWS Trust and Safety, sertakan detail lengkap JSON dari temuan tersebut.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Kredensial yang dibuat secara eksklusif untuk instans EC2 melalui peran peluncuran instans sedang digunakan dari alamat IP eksternal.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail manajemen atau peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa host di luar AWS telah mencoba menjalankan operasi AWS API menggunakan AWS kredensil sementara yang dibuat pada instans EC2 di lingkungan Anda. AWS Instans EC2 yang terdaftar mungkin dikompromikan, dan kredensional sementara dari instance ini mungkin telah diekstraksi ke host jarak jauh di luar. AWS AWS tidak merekomendasikan untuk mendistribusikan ulang kredensi sementara di luar entitas yang membuatnya (misalnya, AWS aplikasi, EC2, atau Lambda). Namun, pengguna yang berwenang dapat mengekspor kredensial dari instans EC2 mereka untuk membuat panggilan API yang sah. Untuk mencegah potensi serangan dan memverifikasi keabsahan aktivitas tersebut, lakukan validasi bahwa penggunaan kredensial instans dari IP jarak jauh dalam temuan tersebut memang diharapkan.

> **Note**
>
> Jika GuardDuty mengamati aktivitas lanjutan dari host jarak jauh, model pembelajaran mesin (ML) akan mengidentifikasi ini sebagai perilaku yang diharapkan. Oleh karena itu, GuardDuty akan berhenti menghasilkan temuan ini untuk aktivitas dari host jarak jauh itu. GuardDuty akan terus menghasilkan temuan untuk perilaku baru dari host jarak jauh lainnya dan akan mengevaluasi kembali host jarak jauh yang dipelajari saat perilaku berubah seiring waktu.

Rekomendasi perbaikan:

Temuan ini dibuat saat jaringan dikonfigurasi untuk merutekan lalu lintas internet sedemikian rupa sehingga keluar dari gateway on-premise, bukan dari Gateway Internet VPC (IGW). Konfigurasi umum, seperti penggunaan AWS Outposts, atau koneksi VPN VPC, dapat mengakibatkan lalu lintas dirutekan dengan cara ini. Jika ini adalah perilaku yang diharapkan, kami sarankan Anda menggunakan aturan penekanan dan membuat aturan yang terdiri dari dua kriteria filter. Kriteria pertama adalah tipe temuan, yaitu `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Kriteria filter kedua adalah Alamat IPv4 pemanggil API dengan alamat IP atau rentang CIDR dari gateway internet lokal Anda. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat Aturan penindasan di GuardDuty.

> **Note**
>
> Jika GuardDuty mengamati aktivitas lanjutan dari sumber eksternal, model pembelajaran mesinnya akan mengidentifikasi ini sebagai perilaku yang diharapkan dan berhenti menghasilkan temuan ini untuk aktivitas dari sumber itu. GuardDuty akan terus menghasilkan temuan untuk perilaku baru dari sumber lain, dan akan mengevaluasi kembali sumber yang dipelajari saat perilaku berubah seiring waktu.

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi, lihat Memperbaiki potensi terganggu AWS credentials.

UnauthorizedAccess:IAMUser/MaliciousIPCaller

API dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa sebuah operasi API (misalnya, percobaan untuk meluncurkan instans EC2, membuat pengguna IAM baru, atau memodifikasi hak akses AWS Anda) diinvokasi dari alamat IP berbahaya yang telah diketahui. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya dalam lingkungan Anda.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

API diinvokasi dari alamat IP pada daftar ancaman kustom.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa operasi API (misalnya, upaya untuk meluncurkan instans EC2, membuat pengguna IAM baru, atau memodifikasi AWS hak istimewa) dipanggil dari alamat IP yang disertakan pada daftar ancaman yang Anda unggah. Dalam GuardDuty, daftar ancaman terdiri dari alamat IP berbahaya yang diketahui. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya dalam lingkungan Anda.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS

Kredensi yang dibuat khusus untuk AWS Tugas Amazon ECS atau AWS Fungsi Lambda sedang digunakan dari akun lain di dalamnya AWS

Tingkat keparahan default: Tinggi*

> **Note**
>
> Tingkat keparahan default temuan ini adalah Tinggi. Namun, jika API dipanggil oleh akun yang berafiliasi dengan AWS lingkungan Anda, tingkat keparahannya adalah Medium.

- Sumber data: peristiwa CloudTrail manajemen atau peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda kapan kredensi tugas AWS Amazon ECS atau kredensi fungsi AWS Lambda Anda digunakan untuk memanggil API dari alamat IP atau titik akhir VPC Amazon, yang

dimiliki oleh akun yang AWS berbeda dari akun yang digunakan sumber daya terkait. Deteksi titik akhir VPC hanya tersedia untuk layanan yang mendukung peristiwa aktivitas jaringan untuk titik akhir VPC. Untuk informasi tentang layanan yang mendukung peristiwa aktivitas jaringan untuk titik akhir VPC, lihat Mencatat log peristiwa aktivitas jaringan di Panduan Pengguna AWS CloudTrail .

AWS tidak merekomendasikan untuk mendistribusikan ulang kredensi sementara di luar entitas yang membuatnya (misalnya, aplikasi, AWS Amazon EC2, atau Amazon Elastic Container Service). Namun, pengguna yang berwenang dapat mengekspor kredensional dari sumber daya mereka untuk melakukan panggilan API yang sah. Jika `remoteAccountDetails.affiliated` `True` bidangnya berarti API dipanggil dari akun yang terkait dengan akun administrator yang sama. Untuk mengesampingkan potensi serangan dan memverifikasi legitimasi aktivitas, hubungi Akun AWS pemilik atau kepala IAM kepada siapa kredensi ini diberikan.

> **Note**
>
> Jika GuardDuty mengamati aktivitas lanjutan dari akun jarak jauh, model pembelajaran mesin (ML) akan mengidentifikasi ini sebagai perilaku yang diharapkan. Oleh karena itu, GuardDuty akan berhenti menghasilkan temuan ini untuk aktivitas dari akun jarak jauh itu. GuardDuty akan terus menghasilkan temuan untuk perilaku baru dari akun jarak jauh lainnya dan akan mengevaluasi kembali akun jarak jauh yang dipelajari saat perilaku berubah seiring waktu.

> **Note**
>
> Untuk tugas Amazon ECS, kredensional dikaitkan dengan peran tugas dan deteksi berlaku terlepas dari konfigurasi VPC.

Rekomendasi perbaikan:

Temuan ini akan dihasilkan ketika permintaan AWS API dibuat di dalam AWS melalui sumber daya di luar Anda Akun AWS, dengan menggunakan kredenal tugas AWS Amazon ECS atau kredenal fungsi Lambda AWS . Mungkin lazim, seperti untuk arsitektur Transit Gateway dalam konfigurasi hub dan spoke, untuk merutekan lalu lintas melalui AWS VPC jalan keluar hub tunggal dengan titik akhir layanan. Jika ini adalah perilaku yang diharapkan, kami sarankan Anda menggunakan Aturan penekanan dengan jenis pencarian kriteria filter, yang seharusnyaUnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS.

Untuk menanggapi temuan ini, Anda dapat menggunakan alur kerja berikut untuk menentukan tindakan:

1. Identifikasi akun jarak jauh yang terlibat dari bidang `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Tentukan apakah akun itu berafiliasi dengan GuardDuty lingkungan Anda dari `service.action.awsApiCallAction.remoteAccountDetails.affiliated` lapangan.
3. Jika akun tersebut berafiliasi, hubungi pemilik akun jarak jauh dan pemilik kredensi sumber daya untuk menyelidiki.

   Jika akun tidak berafiliasi, maka langkah pertama adalah mengevaluasi apakah akun tersebut terkait dengan organisasi Anda tetapi bukan bagian dari pengaturan lingkungan beberapa GuardDuty akun Anda, atau jika GuardDuty belum diaktifkan di akun ini. Selanjutnya, hubungi pemilik kredenal sumber daya untuk menentukan apakah ada kasus penggunaan untuk akun jarak jauh untuk menggunakan kredensi ini.
4. Jika pemilik kredensial tidak mengenali akun jarak jauh tersebut, kredensial mungkin telah disusupi oleh pelaku ancaman yang beroperasi di dalam AWS. Anda harus mengambil langkah-langkah yang direkomendasikanMemperbaiki cluster ECS yang berpotensi dikompromikan, untuk mengamankan lingkungan Anda.

   Selain itu, Anda dapat mengirimkan laporan penyalahgunaan ke tim AWS Trust and Safety untuk memulai penyelidikan ke akun jarak jauh. Saat mengirimkan laporan Anda ke AWS Trust and Safety, sertakan detail lengkap JSON dari temuan tersebut.

UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS

Kredensi yang dibuat khusus untuk AWS sumber daya, (fungsi Lambda atau tugas Amazon ECS), sedang digunakan dari alamat IP di luar AWS.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail manajemen atau peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa host di luar AWS berusaha menjalankan operasi AWS API menggunakan AWS kredensil sementara yang dibuat pada sumber daya AWS (fungsi Lambda atau tugas Amazon ECS) di lingkungan Anda. AWS Sumber daya yang terdaftar mungkin dikompromikan,

dan kredensional sementara dari sumber daya ini mungkin telah diekstraksi ke host jarak jauh di luar. AWS

AWS tidak merekomendasikan untuk mendistribusikan ulang kredensi sementara di luar entitas yang membuatnya (misalnya, aplikasi AWS seperti Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service, atau). AWS Lambda Namun, pengguna yang berwenang dapat mengekspor kredensional dari sumber daya mereka untuk melakukan panggilan API yang sah. Untuk mengesampingkan serangan potensial dan memverifikasi legitimasi aktivitas, validasi jika penggunaan kredensil sumber daya dari IP jarak jauh dalam temuan diharapkan.

> **Note**
>
> Jika GuardDuty mengamati aktivitas lanjutan dari host jarak jauh, model pembelajaran mesin (ML) akan mengidentifikasi ini sebagai perilaku yang diharapkan. Oleh karena itu, GuardDuty akan berhenti menghasilkan temuan ini untuk aktivitas dari host jarak jauh itu. GuardDuty akan terus menghasilkan temuan untuk perilaku baru dari host jarak jauh lainnya dan akan mengevaluasi kembali host jarak jauh yang dipelajari saat perilaku berubah seiring waktu.

Rekomendasi perbaikan:

Temuan ini dihasilkan saat jaringan dikonfigurasi untuk merutekan lalu lintas internet sedemikian rupa sehingga keluar dari gateway on-premise, bukan dari Gateway Internet VPC (IGW). Konfigurasi umum, seperti penggunaan AWS Outposts atau koneksi VPN VPC, dapat mengakibatkan lalu lintas dirutekan dengan cara ini. Jika ini adalah perilaku yang diharapkan, maka GuardDuty rekomendasikan penggunaan Aturan penekanan untuk membuat aturan dengan kriteria dua filter. Kriteria pertama adalah tipe temuan, yang berisi `UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS`. Kriteria filter kedua adalah Alamat IPv4 pemanggil API dengan alamat IP atau rentang CIDR untuk gateway internet on-premise Anda.

Jika aktivitas ini di luar ekspektasi, kredensial Anda mungkin telah disusupi. Untuk informasi tentang langkah-langkah untuk memulihkan jenis temuan ini, lihatMemperbaiki potensi terganggu AWS credentials, atauMemperbaiki cluster ECS yang berpotensi dikompromikan.

UnauthorizedAccess:IAMUser/TorIPCaller

API diinvokasi dari alamat IP simpul keluar Tor.

Tingkat keparahan default: Medium

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa operasi API (misalnya, percobaan untuk meluncurkan instans EC2, membuat pengguna IAM baru, atau mengubah hak akses AWS) diinvokasi dari alamat IP simpul keluar Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Simpul Tor terakhir disebut sebagai simpul keluar. Hal ini dapat mengindikasikan akses yang tidak sah ke sumber daya AWS Anda dengan maksud menyembunyikan identitas penyerang yang sebenarnya.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Lihat informasi yang lebih lengkap di Memperbaiki potensi terganggu AWS credentials.

GuardDuty jenis pencarian urutan serangan

GuardDuty mendeteksi urutan serangan ketika urutan tertentu dari beberapa tindakan selaras dengan aktivitas yang berpotensi mencurigakan. Urutan serangan mencakup sinyal seperti aktivitas dan GuardDuty temuan API. Ketika GuardDuty mengamati sekelompok sinyal dalam urutan tertentu yang menunjukkan ancaman keamanan yang sedang berlangsung, sedang berlangsung, atau baru-baru ini, GuardDuty menghasilkan temuan urutan serangan. GuardDuty menganggap aktivitas API individu weak signals karena mereka tidak menampilkan diri sebagai ancaman potensial.

Deteksi urutan serangan berfokus pada potensi kompromi data Amazon S3 (yang dapat menjadi bagian dari serangan ransomware yang lebih luas), AWS kredenSIAL yang dikompromikan, cluster Amazon EKS yang dikompromikan, cluster Amazon ECS yang dikompromikan, dan grup instans Amazon EC2 yang dikompromikan. Bagian berikut memberikan rincian tentang masing-masing urutan serangan.

Topik

- AttackSequence:EKS/CompromisedCluster
- AttackSequence:ECS/CompromisedCluster
- AttackSequence:EC2/CompromisedInstanceGroup
- AttackSequence:IAM/CompromisedCredentials
- AttackSequence:S3/CompromisedData

AttackSequence:EKS/CompromisedCluster

Urutan tindakan mencurigakan yang dilakukan oleh cluster Amazon EKS yang berpotensi dikompromikan.

- Tingkat keparahan default: Kritis
- Sumber data:
  - Peristiwa log audit EKS
  - Pemantauan Runtime untuk Amazon EKS
  - Deteksi malware Amazon EKS untuk Amazon EC2
  - AWS CloudTrail peristiwa data untuk S3
  - AWS CloudTrail acara manajemen
  - Log Alur VPC
  - Log kueri DNS Route53 Resolver

Temuan ini memberi tahu Anda bahwa GuardDuty mendeteksi urutan tindakan mencurigakan yang menunjukkan cluster Amazon EKS yang berpotensi dikompromikan di lingkungan Anda. Beberapa perilaku serangan mencurigakan dan anomali, seperti proses berbahaya atau koneksi dengan titik akhir berbahaya, diamati di cluster Amazon EKS yang sama.

GuardDuty menggunakan algoritma korelasi kepemilikannya untuk mengamati dan mengidentifikasi urutan tindakan yang dilakukan dengan menggunakan kredensi IAM. GuardDuty mengevaluasi temuan di seluruh rencana perlindungan dan sumber sinyal lainnya untuk mengidentifikasi pola serangan umum dan yang muncul. GuardDuty menggunakan beberapa faktor untuk memunculkan ancaman, seperti reputasi IP, urutan API, konfigurasi pengguna, dan sumber daya yang berpotensi terkena dampak.

Tindakan remediasi: Jika perilaku ini tidak terduga di lingkungan Anda, maka cluster Amazon EKS Anda mungkin terganggu. Untuk panduan remediasi komprehensif, lihat Memperbaiki temuan Perlindungan EKS danMemperbaiki temuan Pemantauan Runtime.

Selain itu, karena AWS kredenSIAL mungkin telah dikompromikan melalui cluster EKS, lihatMemperbaiki potensi terganggu AWS credentials. Untuk langkah-langkah untuk memperbaiki sumber daya lain yang mungkin berpotensi terkena dampak, lihatMemperbaiki temuan GuardDuty keamanan yang terdeteksi.

AttackSequence:ECS/CompromisedCluster

Urutan tindakan mencurigakan yang dilakukan oleh cluster Amazon ECS yang berpotensi dikompromikan.

- Tingkat keparahan default: Kritis
- Sumber data:
  - Pemantauan Runtime untuk Amazon ECS Fargate
  - Pemantauan Runtime untuk Instans EC2 di Amazon ECS
  - GuardDuty Perlindungan Malware untuk Amazon EC2

Temuan ini memberi tahu Anda bahwa GuardDuty mendeteksi urutan sinyal mencurigakan yang menunjukkan cluster Amazon ECS yang berpotensi dikompromikan di lingkungan Anda. Sinyal ini mungkin termasuk proses berbahaya, komunikasi dengan titik akhir berbahaya, atau perilaku penambangan cryptocurrency.

GuardDuty menggunakan algoritma korelasi eksklusif dan beberapa faktor deteksi untuk mengidentifikasi urutan tindakan mencurigakan dalam cluster Amazon ECS. Melalui analisis di seluruh rencana perlindungan dan berbagai sumber sinyal, GuardDuty mengidentifikasi pola serangan umum dan yang muncul, memberikan deteksi keyakinan tinggi terhadap potensi kompromi.

Tindakan remediasi: Jika perilaku ini tidak terduga di lingkungan Anda, cluster Amazon ECS Anda mungkin terganggu. Untuk rekomendasi penahanan ancaman, lihatMemperbaiki cluster ECS yang berpotensi dikompromikan. Perhatikan bahwa kompromi dapat meluas ke satu atau lebih tugas ECS atau beban kerja kontainer, yang dapat digunakan untuk membuat atau memodifikasi AWS sumber daya. Untuk panduan remediasi komprehensif yang mencakup sumber daya yang berpotensi terkena dampak, lihatMemperbaiki temuan GuardDuty keamanan yang terdeteksi.

AttackSequence:EC2/CompromisedInstanceGroup

Urutan tindakan mencurigakan yang menunjukkan instans Amazon EC2 yang berpotensi dikompromikan.

- Tingkat keparahan default: Kritis
- Sumber data:
  - Pemantauan Runtime untuk Amazon EC2

- Deteksi malware untuk Amazon EC2
- Log Alur VPC
- Log kueri DNS Route53 Resolver

Temuan ini menunjukkan GuardDuty terdeteksi urutan tindakan mencurigakan yang menunjukkan potensi kompromi di seluruh grup instans Amazon EC2 di lingkungan Anda. Grup instans biasanya mewakili aplikasi yang dikelola melalui infrastruktur-as-code, berbagi konfigurasi serupa seperti Auto-scaling grup, peran profil instans IAM, tumpukan, template peluncuran Amazon EC AWS CloudFormation 2, AMI atau ID VPC. GuardDuty mengamati beberapa perilaku mencurigakan di satu atau lebih contoh, termasuk:

- Proses berbahaya
- File berbahaya
- Koneksi jaringan yang mencurigakan
- Aktivitas penambangan cryptocurrency
- Penggunaan kredensional instans Amazon EC2 yang mencurigakan

Metode Deteksi: GuardDuty menggunakan algoritma korelasi eksklusif untuk mengidentifikasi urutan tindakan yang mencurigakan dalam instans Amazon EC2. Dengan mengevaluasi temuan di seluruh rencana perlindungan dan berbagai sumber sinyal, GuardDuty mengidentifikasi pola serangan menggunakan berbagai faktor seperti IP dan reputasi domain dan proses yang mencurigakan yang berjalan.

Tindakan remediasi: Jika perilaku ini tidak terduga di lingkungan Anda, instans Amazon EC2 Anda mungkin terganggu. Kompromi dapat melibatkan:

- Beberapa proses
- Kredentif instans yang mungkin telah digunakan untuk memodifikasi instans Amazon EC2 atau sumber daya lainnya AWS

Untuk rekomendasi penahanan ancaman, lihatMemperbaiki instans Amazon EC2 yang berpotensi dikompromikan. Perhatikan bahwa kompromi dapat meluas ke satu atau lebih instans Amazon EC2 dan melibatkan proses yang dikompromikan atau kredentif instans yang dapat digunakan untuk membuat atau memodifikasi instans Amazon EC2 atau sumber daya lainnya AWS . Untuk

panduan remediasi komprehensif yang mencakup sumber daya yang berpotensi terkena dampak, lihatMemperbaiki temuan GuardDuty keamanan yang terdeteksi.

AttackSequence:IAM/CompromisedCredentials

Urutan permintaan API yang dipanggil dengan menggunakan yang berpotensi dikompromikan AWS kredenSIAL.

- Tingkat keparahan default: Kritis
- Sumber data: AWS CloudTrail acara manajemen

Temuan ini memberi tahu Anda bahwa GuardDuty mendeteksi urutan tindakan mencurigakan yang dilakukan dengan menggunakan AWS kredenSIAL yang memengaruhi satu atau lebih sumber daya di lingkungan Anda. Beberapa perilaku serangan mencurigakan dan anomali diamati oleh kredenSIAL yang sama, menghasilkan keyakinan yang lebih tinggi bahwa kredenSIAL disalahgunakan.

GuardDuty menggunakan algoritma korelasi kepemilikannya untuk mengamati dan mengidentifikasi urutan tindakan yang dilakukan dengan menggunakan kredensi IAM. GuardDuty mengevaluasi temuan di seluruh rencana perlindungan dan sumber sinyal lainnya untuk mengidentifikasi pola serangan umum dan yang muncul. GuardDuty menggunakan beberapa faktor untuk memunculkan ancaman, seperti reputasi IP, urutan API, konfigurasi pengguna, dan sumber daya yang berpotensi terkena dampak.

Ketika Anda mengaktifkanPerlindungan AI, juga GuardDuty dapat memasukkan Jenis penemuan Perlindungan AI di antara sinyal yang berkorelasi untuk urutan serangan ini. Temuan ini terkait dengan identitas IAM. Akibatnya, GuardDuty dapat memunculkannya sebagai sinyal dalam urutan serangan ini dan menghubungkannya dengan tindakan mencurigakan lainnya yang diambil dengan kredenSIAL yang berpotensi dikompromikan yang sama. Misalnya, GuardDuty dapat mengkorelasikan sinyal lain dengan pemanggilan model Amazon Bedrock atau Amazon SageMaker AI yang anomali yang dibuat dengan kredenSIAL tersebut, dan memasukkannya ke dalam urutan serangan ini. Dengan sendirinya, temuan Perlindungan AI tidak menghasilkan urutan serangan. Untuk informasi selengkapnya, lihat Perlindungan AI.

Tindakan remediasi: Jika perilaku ini tidak terduga di lingkungan Anda, maka kredensibilitas Anda AWS mungkin telah dikompromikan. Untuk langkah-langkah untuk memperbaiki, lihatMemperbaiki potensi terganggu AWS credentials. KredenSIAL yang dikompromikan mungkin telah digunakan

untuk membuat atau memodifikasi sumber daya tambahan, seperti bucket Amazon S3, AWS Lambda fungsi, atau instans Amazon EC2, di lingkungan Anda. Untuk langkah-langkah untuk memperbaiki sumber daya lain yang mungkin berpotensi terkena dampak, lihatMemperbaiki temuan GuardDuty keamanan yang terdeteksi.

AttackSequence:S3/CompromisedData

Urutan permintaan API dipanggil dalam upaya potensial untuk mengeksfiltrasi atau menghancurkan data di Amazon S3.

- Tingkat keparahan default: Kritis
- Sumber data: AWS CloudTrail peristiwa data untuk S3 dan AWS CloudTrail acara manajemen

Temuan ini memberi tahu Anda bahwa GuardDuty mendeteksi urutan tindakan mencurigakan yang menunjukkan kompromi data dalam satu atau beberapa bucket Amazon Simple Storage Service (Amazon S3), dengan menggunakan kredenSIAL yang berpotensi dikompromik AWS an. Beberapa perilaku serangan mencurigakan dan anomali (permintaan API) diamati, yang mengakibatkan kepercayaan yang lebih tinggi dari kredenSIAL yang disalahgunakan.

GuardDuty menggunakan algoritma korelasinya untuk mengamati dan mengidentifikasi urutan tindakan yang dilakukan dengan menggunakan kredensi IAM. GuardDuty kemudian mengevaluasi temuan di seluruh rencana perlindungan dan sumber sinyal lainnya untuk mengidentifikasi pola serangan umum dan yang muncul. GuardDuty menggunakan beberapa faktor untuk memunculkan ancaman, seperti reputasi IP, urutan API, konfigurasi pengguna, dan sumber daya yang berpotensi terkena dampak.

Tindakan remediasi: Jika aktivitas ini tidak terduga di lingkungan Anda, AWS kredenSIAL, atau data Amazon S3 Anda mungkin berpotensi dieksfiltrasi atau dihancurkan. Untuk langkah-langkah untuk memperbaiki, lihat Memperbaiki potensi terganggu AWS credentials danMemperbaiki bucket S3 yang berpotensi dikompromikan.

Jenis pencarian Aturan Deteksi Kustom

Halaman ini mencantumkan jenis temuan yang GuardDuty dihasilkan dari Aturan Deteksi Kustom, dikelompokkan berdasarkan sumber data. Setiap jenis temuan menggabungkan satu atau lebih sinyal menjadi satu temuan. Untuk informasi selengkapnya tentang mengaktifkan Aturan Deteksi Kustom, lihatAturan Deteksi Kustom di GuardDuty.

> **Note**
>
> Aturan individu hanya tersedia dalam Wilayah AWS mendukung AWS layanan atau fitur yang mereka targetkan. Misalnya, aturan yang menargetkan AWS Organizations atau Amazon Simple Email Service hanya tersedia di Wilayah tempat layanan tersebut beroperasi. Demikian pula, aturan yang menargetkan URL fungsi Lambda atau instance notebook SageMaker AI hanya tersedia di Wilayah di mana fitur tersebut didukung.

Topik

- Aturan Deteksi Kustom untuk AWS CloudTrail acara manajemen
- Aturan Deteksi Kustom untuk Pemantauan Runtime

Aturan Deteksi Kustom untuk AWS CloudTrail acara manajemen

Jenis temuan berikut dihasilkan dari sinyal acara AWS CloudTrail manajemen, yang diselenggarakan oleh taktik MITRE ATT&CK®.

Akses Kredensi

Aturan ini mencoba mendeteksi operasi yang mengambil atau mengatur ulang kredensyal, seperti mengambil kata sandi instans Amazon EC2 atau menyetel ulang kata sandi administrator Amazon RDS.

Tipe temuan	Nama aturan	Kepelikan
CredentialAccess:EC2/UnsecuredCredentials	EC2PasswordDataRetrieved	MEDIUM
CredentialAccess:RDS/ModifyAuthenticationProcess	RDSMasterPasswordReset	TINGGI

Gangguan Pertahanan

Aturan ini mencoba mendeteksi perubahan yang menonaktifkan atau melemahkan kontrol keamanan, seperti menghapus log aliran VPC, menonaktifkan kebijakan organisasi, atau menghapus akun dari organisasi.

Tipe temuan	Nama aturan	Kepelikan
DefenseImpairment:EC2/DisableOrModifyTools	EC2TerminationProtectionEnabled	RENDAH
	VPCFlowLogsDeleted	TINGGI
DefenseImpairment:Organizations/ModifyCloudResourceHierarchy	OrganizationLeaveAttempt	TINGGI
DefenseImpairment:Organizations/DisableOrModifyTools	OrganizationPolicyDisabled	TINGGI
DefenseImpairment:RDS/ModifyAuthenticationProcess	RDSIAMAuthDisabled	MEDIUM
DefenseImpairment:Route53Resolver/DisableOrModifyTools	DNSQueryLogsDeleted	MEDIUM
DefenseImpairment:S3/DisableOrModifyTools	S3CustomerProvidedKeysEnabled	TINGGI

Eksekusi

Aturan ini mencoba mendeteksi perubahan yang menjalankan kode pada sumber daya, seperti memodifikasi konfigurasi siklus hidup notebook SageMaker AI.

Tipe temuan	Nama aturan	Kepelikan
Execution:SageMaker/CommandAndScriptingInterpreter	SageMakerLifecycleConfigModified	MEDIUM

Exfiltrasi

Aturan ini mencoba mendeteksi perubahan yang berbagi sumber daya di luar akun Anda, seperti membuat snapshot AMI, Amazon EBS, atau snapshot Amazon RDS dapat diakses oleh akun lain.

Tipe temuan	Nama aturan	Kepelikan
Exfiltration:EC2/TransferDataToCloudAccount	AMIExternalAccess	TINGGI
	EBSSnapshotExternalAccess	TINGGI
Exfiltration:RDS/TransferDataToCloudAccount	RDSSnapshotPubliclyShared	TINGGI
Exfiltration:S3/TransferDataToCloudAccount	S3BucketPolicyExternalAccess	TINGGI

Dampak

Aturan ini mencoba mendeteksi perubahan yang dapat mengganggu atau menghancurkan data dan sumber daya, seperti menyetel objek Amazon S3 agar kedaluwarsa dengan cepat, atau mengaktifkan pengiriman Amazon SES.

Tipe temuan	Nama aturan	Kepelikan
Impact:S3/DataDestruction	S3LifecycleRapidExpiration	MEDIUM
Impact:SES/ResourceHijacking	SESAccountSendingEnabled	RENDAH
	SESProductionAccessEnabled	MEDIUM

Akses Awal

Aturan ini mencoba mendeteksi aktivitas yang membuka akses ke lingkungan Anda, seperti login konsol tanpa MFA atau membuat database Amazon RDS dapat diakses publik.

Tipe temuan	Nama aturan	Kepelikan
InitialAccess:IAM/ValidAccounts	ConsoleLoginWithoutMFA	MEDIUM
InitialAccess:RDS/ExploitPublicFacingApplication	RDSPubliclyAccessible	TINGGI

Gerakan Lateral

Aturan ini mencoba mendeteksi aktivitas yang memberikan akses antar sumber daya, seperti mendorong kunci SSH ke instans Amazon EC2.

Tipe temuan	Nama aturan	Kepelikan
LateralMovement:EC2/RemoteServices	EC2InstanceSSHKeyPushed	MEDIUM

Tetap

Aturan ini mencoba mendeteksi perubahan yang membuat atau memperluas akses, seperti membuat kunci akses IAM, memodifikasi kebijakan kepercayaan peran, atau membuat fungsi Lambda dapat diakses publik.

Tipe temuan	Nama aturan	Kepelikan
Persistence:EC2/BootOrLogonInitializationScripts	EC2UserDataModified	TINGGI
Persistence:EC2/ExternalRemoteServices	EC2SecurityGroupPublicSSH	MEDIUM
Persistence:IAM/AccountManipulation	IAMAccessKeyCreated	RENDAH
	IAMRoleTrustPolicyModified	MEDIUM
	IAMUserLoginProfileCreated	TINGGI
	IAMUserLoginProfileUpdated	MEDIUM
Persistence:Lambda/AccountManipulation	LambdaFunctionPublicAccess	TINGGI
Persistence:Lambda/ModifyAuthenticationProcess	LambdaFunctionUrlPublicAccess	TINGGI
Persistence:RolesAnywhere/AccountManipulation	RolesAnywhereTrustAnchorCreated	MEDIUM

Eskalasi Hak Istimewa

Aturan ini mencoba mendeteksi perubahan yang memberikan izin yang lebih luas, seperti melampirkan kebijakan administrator ke pengguna atau peran IAM.

Tipe temuan	Nama aturan	Kepelikan
PrivilegeEscalation:IAM/AccountManipulation	AdminPolicyAttachedToRole	TINGGI
	AdminPolicyAttachedToUser	TINGGI
	BedrockServiceCredentialCreated	MEDIUM
	SESFullAccessPolicyAttached ToRole	MEDIUM
	SESFullAccessPolicyAttached ToUser	MEDIUM

Pengembangan Sumber Daya

Aturan ini mencoba mendeteksi penyiapan sumber daya yang dapat mendukung aktivitas selanjutnya, seperti memverifikasi identitas domain Amazon SES.

Tipe temuan	Nama aturan	Kepelikan
ResourceDevelopment:SES/CompromiseAccounts	SESDomainIdentityVerified	MEDIUM

Aturan Deteksi Kustom untuk Pemantauan Runtime

GuardDuty menghasilkan tipe pencarian Aturan Deteksi Kustom berikut dari sinyal Runtime Monitoring, yang diatur berdasarkan taktik MITRE ATT&CK®. Aturan ini memerlukan Runtime Monitoring dan agen GuardDuty keamanan pada sumber daya yang dipantau. Untuk informasi selengkapnya, lihat Sumber data dan sinyal.

Perintah dan Kontrol

Aturan ini mencoba mendeteksi proses lalu lintas jaringan terowongan, seperti alat tunneling DNS atau terowongan protokol.

Tipe temuan	Nama aturan	Kepelikan
CommandAndControl:Runtime/SuspiciousCommand	DnsTunnelingToolExecuted	TINGGI
CommandAndControl:Runtime/SuspiciousCommand	SuspiciousProtocolTunneling	MEDIUM

Akses Kredensi

Aturan ini mencoba mendeteksi proses yang membaca data sensitif, seperti memori proses melalui sistem `/proc` file.

Tipe temuan	Nama aturan	Kepelikan
CredentialAccess:Runtime/SensitiveFileRead	DumpProcessMemoryFromProc	TINGGI

Gangguan Pertahanan

Aturan ini mencoba mendeteksi proses yang melemahkan pertahanan host, seperti menonaktifkan pencatatan audit, memodifikasi aturan firewall, atau menghentikan layanan.

Tipe temuan	Nama aturan	Kepelikan
DefenseEvasion:Runtime/SensitiveFileModified	FirewallConfigModified	MEDIUM
DefenseEvasion:Runtime/SensitiveFileModified	LogManipulation	MEDIUM
DefenseEvasion:Runtime/SuspiciousCommand	AuditDisabled	MEDIUM
DefenseEvasion:Runtime/SuspiciousCommand	FirewallDisablement	MEDIUM
DefenseEvasion:Runtime/SuspiciousCommand	KernelHardeningDisabled	MEDIUM

Tipe temuan	Nama aturan	Kepelikan
DefenseEvasion:Runtime/SuspiciousCommand	KillCommandUsage	MEDIUM
DefenseEvasion:Runtime/SuspiciousCommand	ServiceStoppedOrDisabled	MEDIUM

Penemuan

Aturan ini mencoba mendeteksi proses yang mengumpulkan informasi tentang sumber daya, seperti membaca file kata sandi, mencari kredensi atau kunci, atau mendeteksi virtualisasi.

Tipe temuan	Nama aturan	Kepelikan
Discovery:Runtime/SensitiveFileRead	PasswordShadowFileDiscovery	MEDIUM
Discovery:Runtime/SuspiciousCommand	FindCommandReconCloudCredentials	MEDIUM
Discovery:Runtime/SuspiciousCommand	FindCommandReconKeyMaterial	MEDIUM
Discovery:Runtime/SuspiciousCommand	PromiscuousModeEnabled	MEDIUM
Discovery:Runtime/SuspiciousCommand	SSHWithHostKeyCheckingDisabled	MEDIUM
Discovery:Runtime/SuspiciousCommand	SqliteDatabaseDump	RENDAH
Discovery:Runtime/SuspiciousCommand	VirtualizationDetection	RENDAH

Eksekusi

Aturan ini mencoba mendeteksi proses yang menjalankan perintah atau kode yang mungkin berbahaya, seperti mengunduh dan menjalankan skrip atau membuka shell interaktif dalam wadah.

Tipe temuan	Nama aturan	Kepelikan
Execution:Runtime/SuspiciousCommand	ChmodInTmpDirectory	MEDIUM

Tipe temuan	Nama aturan	Kepelikan
Execution:Runtime/SuspiciousCommand	CurlWgetScriptDownload	MEDIUM
Execution:Runtime/SuspiciousCommand	DataEncryptionUsingCommandLineUtilities	MEDIUM
Execution:Runtime/SuspiciousCommand	InlinePythonExecution	MEDIUM
Execution:Runtime/SuspiciousCommand	InteractiveShellInsideAContainer	MEDIUM
Execution:Runtime/SuspiciousCommand	RemoteFileCopy	MEDIUM
Execution:Runtime/SuspiciousCommand	ShellFromUtilities	MEDIUM
Execution:Runtime/SuspiciousTool	NetworkSnifferToolExecuted	MEDIUM
Execution:Runtime/SuspiciousTool	RawSocketCreated	MEDIUM

Exfiltrasi

Aturan ini mencoba mendeteksi proses yang memindahkan data dari sumber daya, seperti mengunggah file dengan curl, wget, atau rclone, atau memisahkan data sebelum transfer.

Tipe temuan	Nama aturan	Kepelikan
Exfiltration:Runtime/SuspiciousCommand	CurlWgetExfiltrateData	MEDIUM
Exfiltration:Runtime/SuspiciousCommand	DataSplittingForExfiltration	MEDIUM
Exfiltration:Runtime/SuspiciousCommand	S3DataExfiltrationWithRclone	MEDIUM

Tetap

Aturan ini mencoba mendeteksi perubahan yang menjaga akses ke sumber daya, seperti memodifikasi akun pengguna, kunci resmi SSH, pekerjaan terjadwal, atau layanan sistem.

Tipe temuan	Nama aturan	Kepelikan
Persistence:Runtime/SensitiveFileModified	PAMConfigModification	MEDIUM
Persistence:Runtime/SensitiveFileModified	PasswordModification	MEDIUM
Persistence:Runtime/SensitiveFileModified	SSHAuthorizedKeysModification	MEDIUM
Persistence:Runtime/SensitiveFileModified	ScheduledJobManipulation	MEDIUM
Persistence:Runtime/SensitiveFileModified	ShellRCFileManipulated	MEDIUM
Persistence:Runtime/SensitiveFileModified	SystemdServiceManipulation	MEDIUM
Persistence:Runtime/SuspiciousCommand	AuditdKeylogger	MEDIUM
Persistence:Runtime/SuspiciousCommand	InteractiveLocalAccountCreation	MEDIUM
Persistence:Runtime/SuspiciousCommand	NobodyUserManipulation	TINGGI
Persistence:Runtime/SuspiciousCommand	SshFromPublicIPAddress	MEDIUM
Persistence:Runtime/SuspiciousCommand	SystemdTransientServiceCreated	MEDIUM

Eskalasi Hak Istimewa

Aturan ini mencoba mendeteksi perubahan yang memberikan izin tingkat yang lebih tinggi, seperti memodifikasi file sudoers, menyetel flag setuid, atau melarikan diri dari wadah dengan nsenter.

Tipe temuan	Nama aturan	Kepelikan
DefenseEvasion:Runtime/SuspiciousCommand	FindCommandReconSetuidSetgidFiles	MEDIUM
PrivilegeEscalation:Runtime/SensitiveFileModified	SudoerFileLinked	MEDIUM
PrivilegeEscalation:Runtime/SensitiveFileModified	SudoerFileManipulation	MEDIUM

Tipe temuan	Nama aturan	Kepelikan
PrivilegeEscalation:Runtime/SensitiveFileModified	SudoerFileRenamed	MEDIUM
PrivilegeEscalation:Runtime/SuspiciousCommand	AddSetUIDCapability	TINGGI
PrivilegeEscalation:Runtime/SuspiciousCommand	NewUserAddedToRootGroup	TINGGI
PrivilegeEscalation:Runtime/SuspiciousCommand	NsenterContainerEscape	TINGGI
PrivilegeEscalation:Runtime/SuspiciousCommand	SetUidFlagSet	MEDIUM
PrivilegeEscalation:Runtime/SuspiciousCommand	SudoPrivilegeEnumeration	MEDIUM
PrivilegeEscalation:Runtime/SuspiciousCommand	SudoerFileRead	MEDIUM

Stealth

Aturan ini mencoba mendeteksi proses yang menyembunyikan aktivitas, seperti membajak fungsi pustaka dengan LD_PRELOAD atau menyandikan data dengan Base64.

Tipe temuan	Nama aturan	Kepelikan
DefenseEvasion:Runtime/SensitiveFileModified	LDPreloadFunctionHijack	MEDIUM
DefenseEvasion:Runtime/SuspiciousCommand	Base64EncodeDecode	MEDIUM
DefenseEvasion:Runtime/SuspiciousCommand	BpftoolProgramLoaded	MEDIUM
DefenseEvasion:Runtime/SuspiciousCommand	DebugfsRawDiskAccess	MEDIUM
DefenseEvasion:Runtime/SuspiciousCommand	SuspiciousExecutionPath	MEDIUM

GuardDuty Jenis temuan perlindungan S3

Temuan berikut ini khusus untuk sumber daya Amazon S3 dan akan memiliki Jenis Sumber Daya `S3Bucket` jika sumber datanya adalah peristiwa CloudTrail data untuk S3, atau `AccessKey` jika sumber datanya adalah peristiwa CloudTrail manajemen. Tingkat kepelikan dan detail temuan akan berbeda berdasarkan tipe temuan dan izin yang terkait dengan bucket.

Temuan yang tercantum di sini termasuk sumber data dan model yang digunakan untuk menghasilkan tipe temuan. Untuk informasi lebih lanjut sumber data dan model, lihatGuardDuty sumber data dasar.

> **Important**
>
> Temuan dengan sumber data peristiwa CloudTrail data untuk S3 hanya dihasilkan jika Anda telah mengaktifkan S3 Protection. Secara default, setelah 31 Juli 2020, Perlindungan S3 diaktifkan saat akun diaktifkan GuardDuty untuk pertama kalinya, atau ketika akun GuardDuty administrator yang didelegasikan mengaktifkan GuardDuty di akun anggota yang ada. Namun, ketika anggota baru bergabung dengan GuardDuty organisasi, preferensi pengaktifan otomatis organisasi akan berlaku. Untuk informasi tentang preferensi mengaktifkan otomatis, lihatMenyetel preferensi aktifkan otomatis organisasi. Untuk informasi tentang cara mengaktifkan S3 Protection, lihat GuardDuty Perlindungan S3

Untuk semua temuan `S3Bucket` jenis, Anda disarankan untuk memeriksa izin pada bucket yang bersangkutan dan izin dari setiap pengguna yang terlibat dalam penemuan, jika aktivitas tidak terduga, lihat rekomendasi remediasi yang dirinci diMemperbaiki bucket S3 yang berpotensi dikompromikan.

Topik

- Discovery:S3/AnomalousBehavior
- Discovery:S3/MaliciousIPCaller
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- Exfiltration:S3/AnomalousBehavior
- Exfiltration:S3/MaliciousIPCaller
- Impact:S3/AnomalousBehavior.Delete

- Impact:S3/AnomalousBehavior.Permission
- Impact:S3/AnomalousBehavior.Write
- Impact:S3/MaliciousIPCaller
- PenTest:S3/KaliLinux
- PenTest:S3/ParrotLinux
- PenTest:S3/PentooLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller

Discovery:S3/AnomalousBehavior

API yang biasa digunakan untuk menemukan objek S3 diinvokasi dengan cara yang beranomali.

Tingkat keparahan default: Rendah

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM telah menginvokasi API S3 untuk menemukan bucket S3 dalam lingkungan Anda, seperti `ListObjects`. Jenis aktivitas ini dikaitkan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah AWS lingkungan Anda rentan terhadap serangan yang lebih luas. Aktivitas ini mencurigakan karena entitas IAM menginvokasi API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya menginvokasi API S3, atau entitas IAM menginvokasi API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML ini mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa

anomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi lebih lanjut tentang faktor-faktor yang membuat permintaan API menjadi tidak biasa untuk identitas pengguna yang menginvokasi permintaan tersebut, lihat Detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Discovery:S3/MaliciousIPCaller

API S3 yang biasa digunakan untuk menemukan sumber daya dalam AWS lingkungan dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3 dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati biasanya dikaitkan dengan tahap penemuan serangan ketika musuh mengumpulkan informasi tentang AWS lingkungan Anda. Contohnya termasuk `GetObjectAcl` dan `ListObjects`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Discovery:S3/MaliciousIPCaller.Custom

API S3 diinvokasi dari alamat IP yang termasuk dalam daftar ancaman kustom.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa API S3, seperti `GetObjectAcl` atau `ListObjects`, diinvokasi dari alamat IP yang termasuk dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi tambahan dari detail temuan ini. Tipe aktivitas ini terkait dengan tahap penemuan serangan ketika penyerang mengumpulkan informasi untuk menentukan apakah lingkungan AWS Anda rentan terhadap serangan yang lebih luas.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Discovery:S3/TorIPCaller

API S3 diinvokasi dari alamat IP simpul keluar Tor.

Tingkat keparahan default: Medium

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa API S3, seperti `GetObjectAcl` atau `ListObjects`, diinvokasi dari alamat IP simpul keluar Tor. Jenis aktivitas ini dikaitkan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah AWS lingkungan Anda rentan terhadap serangan yang lebih luas. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Simpul Tor terakhir disebut sebagai simpul keluar. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Exfiltration:S3/AnomalousBehavior

Entitas IAM memanggil API S3 dengan cara yang mencurigakan.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM membuat panggilan API yang melibatkan bucket S3 dan aktivitas ini berbeda dari baseline yang ditetapkan entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini terkait dengan tahap eksfiltrasi serangan saat penyerang mencoba mengumpulkan data. Aktivitas ini mencurigakan karena entitas IAM menginvokasi API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya menginvokasi API S3, atau entitas IAM menginvokasi API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML ini mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi lebih lanjut tentang faktor-faktor yang membuat permintaan API menjadi tidak biasa untuk identitas pengguna yang menginvokasi permintaan tersebut, lihat Detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Exfiltration:S3/MaliciousIPCaller

S3 API yang biasa digunakan untuk mengumpulkan data dari AWS lingkungan dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3 dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati umumnya berkaitan dengan taktik eksfiltrasi ketika musuh mencoba mengumpulkan data dari jaringan Anda. Contohnya termasuk `GetObject` dan `CopyObject`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Impact:S3/AnomalousBehavior.Delete

Entitas IAM menginvokasi API S3 yang mencoba menghapus data dengan cara yang mencurigakan.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM di AWS lingkungan Anda membuat panggilan API yang melibatkan bucket S3, dan perilaku ini berbeda dari baseline yang ditetapkan entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini dikaitkan dengan serangan yang mencoba menghapus data. Aktivitas ini mencurigakan karena entitas IAM menginvokasi API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya menginvokasi API S3, atau entitas IAM menginvokasi API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML ini mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi lebih lanjut tentang faktor-faktor yang membuat permintaan API menjadi tidak biasa untuk identitas pengguna yang menginvokasi permintaan tersebut, lihat Detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Kami merekomendasikan audit konten bucket S3 Anda untuk menentukan apakah versi objek sebelumnya dapat atau harus dipulihkan.

Impact:S3/AnomalousBehavior.Permission

API yang biasa digunakan untuk menetapkan izin daftar kontrol akses (ACL) diinvokasi dengan cara yang beranomali.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM di AWS lingkungan Anda telah memperbarui kebijakan bucket atau ACL pada bucket S3 yang terdaftar. Perubahan ini dapat mengekspos bucket S3 Anda secara publik ke semua AWS pengguna yang diautentikasi.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML ini mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi lebih lanjut tentang faktor-faktor yang membuat permintaan API menjadi tidak biasa untuk identitas pengguna yang menginvokasi permintaan tersebut, lihat Detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Kami merekomendasikan audit konten bucket S3 Anda untuk memastikan bahwa tidak ada objek yang secara tak terduga diizinkan untuk diakses secara publik.

Impact:S3/AnomalousBehavior.Write

Entitas IAM menginvokasi API S3 yang mencoba menulis data dengan cara yang mencurigakan.

Tingkat keparahan default: Medium

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM di AWS lingkungan Anda membuat panggilan API yang melibatkan bucket S3, dan perilaku ini berbeda dari baseline yang ditetapkan entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini dikaitkan dengan serangan yang mencoba menulis data. Aktivitas ini mencurigakan karena entitas IAM menginvokasi API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya menginvokasi API S3, atau entitas IAM menginvokasi API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML ini mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh penyerang. Model ML ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi lebih lanjut tentang faktor-faktor yang membuat permintaan API menjadi tidak biasa untuk identitas pengguna yang menginvokasi permintaan tersebut, lihat Detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Kami merekomendasikan audit konten bucket S3 Anda untuk memastikan bahwa panggilan API ini tidak menulis data berbahaya atau tidak sah.

Impact:S3/MaliciousIPCaller

API S3 yang biasa digunakan untuk merusak data atau proses dalam sebuah AWS lingkungan dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3 dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati biasanya dikaitkan dengan taktik dampak di mana musuh mencoba memanipulasi, mengganggu, atau menghancurkan data di AWS lingkungan Anda. Contohnya termasuk `PutObject` dan `PutObjectAcl`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

PenTest:S3/KaliLinux

API S3 diinvokasi dari mesin Kali Linux.

Tingkat keparahan default: Medium

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Kali Linux membuat panggilan API S3 menggunakan kredenSIAL milik AWS akun Anda. Kredensial Anda mungkin disusupi. Kali Linux adalah alat uji penetrasi populer yang digunakan para profesional keamanan untuk mengidentifikasi kelemahan dalam instans EC2 yang memerlukan patching. Penyerang juga menggunakan alat ini untuk menemukan kelemahan konfigurasi EC2 dan mendapatkan akses tidak sah ke AWS lingkungan Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

PenTest:S3/ParrotLinux

API S3 diinvokasi dari mesin Parrot Security Linux.

Tingkat keparahan default: Medium

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Parrot Security Linux membuat panggilan API S3 menggunakan kredenSIAL milik AWS akun Anda. Kredensial Anda mungkin disusupi. Parrot Security Linux adalah alat uji penetrasi populer yang digunakan para profesional keamanan untuk mengidentifikasi kelemahan dalam instans EC2 yang memerlukan patching. Penyerang juga menggunakan alat ini untuk menemukan kelemahan konfigurasi EC2 dan memperoleh akses yang tidak sah ke lingkungan AWS Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

PenTest:S3/PentooLinux

API S3 diinvokasi dari mesin Pentoo Linux.

Tingkat keparahan default: Medium

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Pentoo Linux membuat panggilan API S3 menggunakan kredenSIAL milik AWS akun Anda. Kredensial Anda mungkin disusupi. Pentoo Linux adalah alat uji penetrasi populer yang digunakan para profesional keamanan untuk mengidentifikasi kelemahan dalam instans EC2 yang memerlukan patching. Penyerang juga menggunakan alat ini untuk menemukan kelemahan konfigurasi EC2 dan mendapatkan akses tidak sah ke AWS lingkungan Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Policy:S3/AccountBlockPublicAccessDisabled

Entitas IAM memanggil API yang digunakan untuk menonaktifkan Akses Publik Blok S3 pada akun.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa Blokir Akses Publik Amazon S3 dinonaktifkan pada tingkat akun. Ketika pengaturan Blokir Akses Publik S3 diaktifkan, ini digunakan untuk memfilter kebijakan

atau daftar kontrol akses (ACL) pada bucket sebagai tindakan keamanan untuk mencegah eksposur data publik yang tidak disengaja.

Biasanya, Blokir Akses Umum S3 dinonaktifkan pada akun untuk memungkinkan akses publik ke bucket atau ke objek dalam bucket. Ketika Blokir Akses Publik S3 dinonaktifkan pada akun, akses ke bucket Anda dikendalikan oleh kebijakan, ACL, atau pengaturan Blokir Akses Publik tingkat bucket diterapkan ke bucket individu Anda. Hal ini tidak berarti bahwa bucket dibagikan secara publik, tetapi bahwa Anda harus mengaudit izin yang diterapkan ke bucket untuk mengonfirmasi bahwa izin tersebut menyediakan tingkat akses yang sesuai.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Policy:S3/BucketAnonymousAccessGranted

Principal IAM telah memberikan akses ke bucket S3 ke internet dengan mengubah kebijakan bucket atau ACL.

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa bucket S3 yang tercantum telah dibuat agar dapat diakses secara publik di internet karena entitas IAM telah mengubah kebijakan bucket atau ACL pada bucket tersebut.

Setelah perubahan kebijakan atau ACL terdeteksi, GuardDuty gunakan penalaran otomatis yang didukung oleh Zelkova, untuk menentukan apakah bucket dapat diakses publik.

> **Note**
>
> Jika ACL atau kebijakan bucket dikonfigurasi untuk secara eksplisit menolak atau menolak semua, temuan ini mungkin tidak mencerminkan status bucket saat ini. Temuan ini tidak akan mencerminkan set elan Akses Publik Blok S3 yang mungkin telah diaktifkan untuk bucket S3 Anda. Dalam kasus seperti itu, `effectivePermission` nilai dalam temuan akan ditandai sebagai`UNKNOWN`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Policy:S3/BucketBlockPublicAccessDisabled

Entitas IAM memanggil API yang digunakan untuk menonaktifkan Akses Publik Blok S3 pada bucket.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa Blokir Akses Publik dinonaktifkan untuk bucket S3 yan tercantum. Jika diaktifkan, pengaturan Blokir Akses Publik S3 digunakan untuk memfilter kebijakan atau daftar kontrol akses (ACL) yang diterapkan ke bucket sebagai tindakan keamanan untuk mencegah eksposur data publik yang tidak disengaja.

Biasanya, Blokir Akses Publik S3 dinonaktifkan pada bucket untuk memungkinkan akses publik ke bucket atau ke objek di dalamnya. Ketika Blokir Akses Publik S3 dinonaktifkan pada bucket, akses ke bucket dikendalikan oleh kebijakan atau ACL yang diterapkan padanya. Hal ini tidak berarti bahwa bucket dibagikan secara publik, tetapi Anda harus mengaudit kebijakan dan ACL yang diterapkan ke bucket untuk mengonfirmasi bahwa izin yang sesuai diterapkan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Policy:S3/BucketPublicAccessGranted

Prinsipal IAM telah memberikan akses publik ke bucket S3 untuk semua AWS pengguna dengan mengubah kebijakan bucket atau ACL.

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa bucket S3 yang terdaftar telah diekspos secara publik ke semua AWS pengguna yang diautentikasi karena entitas IAM telah mengubah kebijakan bucket atau ACL pada bucket S3 tersebut.

Setelah perubahan kebijakan atau ACL terdeteksi, GuardDuty gunakan penalaran otomatis yang didukung oleh Zelkova, untuk menentukan apakah bucket dapat diakses publik.

> **Note**
>
> Jika ACL atau kebijakan bucket dikonfigurasi untuk secara eksplisit menolak atau menolak semua, temuan ini mungkin tidak mencerminkan status bucket saat ini. Temuan ini tidak akan mencerminkan set elan Akses Publik Blok S3 yang mungkin telah diaktifkan untuk bucket S3 Anda. Dalam kasus seperti itu, `effectivePermission` nilai dalam temuan akan ditandai sebagai`UNKNOWN`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Stealth:S3/ServerAccessLoggingDisabled

Pencatatan log akses server S3 dinonaktifkan untuk bucket.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa logging akses server S3 dinonaktifkan untuk bucket dalam AWS lingkungan Anda. Jika dinonaktifkan, tidak ada log permintaan web yang dibuat untuk setiap upaya mengakses bucket S3 yang diidentifikasi, namun, panggilan API manajemen S3 ke bucket, seperti DeleteBucket, masih dilacak. Jika logging peristiwa data S3 diaktifkan melalui CloudTrail untuk bucket ini, permintaan web untuk objek di dalam bucket masih akan dilacak. Menonaktifkan pencatatan log adalah teknik yang digunakan oleh pengguna yang tidak sah untuk menghindari

deteksi. Untuk mempelajari selengkapnya tentang log S3, lihat Pencatatan Log Akses Server S3 dan Opsi Pencatatan Log S3.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

API S3 diinvokasi dari alamat IP yang termasuk dalam daftar ancaman kustom.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa operasi API S3, seperti `PutObject` atau `PutObjectAcl`, diinvokasi dari alamat IP yang termasuk dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi tambahan dari detail temuan ini.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

UnauthorizedAccess:S3/TorIPCaller

API S3 diinvokasi dari alamat IP simpul keluar Tor.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa operasi API S3, seperti `PutObject` atau `PutObjectAcl`, diinvokasi dari alamat IP simpul keluar Tor. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Simpul Tor terakhir disebut sebagai simpul keluar. Temuan ini

dapat menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Lihat informasi yang lebih lengkap di Memperbaiki bucket S3 yang berpotensi dikompromikan.

Jenis penemuan Perlindungan EKS

Temuan berikut khusus untuk sumber daya Amazon EKS dan memiliki resource_type. `EKSCluster` Tingkat keparahan dan detail temuan berbeda berdasarkan jenis temuan.

Untuk semua temuan jenis log audit EKS, kami sarankan Anda memeriksa sumber daya yang dimaksud untuk menentukan apakah aktivitas tersebut diharapkan atau berpotensi berbahaya. Untuk panduan tentang memulihkan sumber daya log audit EKS yang dikompromikan yang diidentifikasi oleh GuardDuty temuan, lihat. Memperbaiki temuan Perlindungan EKS

> **Note**
>
> Jika aktivitas yang menghasilkan temuan ini diharapkan, pertimbangkan Aturan penindasan di GuardDuty untuk menambahkan untuk mencegah peringatan di masa depan.

Topik

- CredentialAccess:Kubernetes/MaliciousIPCaller
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess
- CredentialAccess:Kubernetes/TorIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom
- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess
- DefenseEvasion:Kubernetes/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller

- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

> **Note**
>
> Sebelum Kubernetes versi 1.14, `system:unauthenticated` grup ini dikaitkan dengan dan secara default. `system:discovery` `system:basic-user` ClusterRoles Asosiasi ini memungkinkan akses yang tidak diinginkan dari pengguna anonim. Pembaruan cluster tidak mencabut izin ini. Bahkan jika Anda memperbarui klaster Anda ke versi 1.14 atau lebih tinggi,

izin ini mungkin masih diaktifkan. Kami menyarankan Anda untuk memisahkan izin ini dari grup. `system:unauthenticated` Untuk panduan tentang mencabut izin ini, lihat Praktik terbaik keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk mengakses kredensial atau rahasia dalam klaster Kubernetes diinvokasi dari alamat IP berbahaya yang telah diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API diinvokasi dari alamat IP yang terkait dengan aktivitas berbahaya yang telah diketahui. API yang diamati biasanya dikaitkan dengan taktik akses kredenal di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk klaster Kubernetes Anda.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

API yang biasa digunakan untuk mengakses kredensial atau rahasia dalam klaster Kubernetes diinvokasi dari alamat IP yang disertakan di daftar ancaman kustom.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API diinvokasi dari alamat IP yang disertakan di daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan ini. API yang diamati biasanya dikaitkan dengan taktik akses kredenal di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk klaster Kubernetes Anda.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *`KubernetesUserDetails`* bagian ini adalah*`system:anonymous`*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

API yang biasa digunakan untuk mengakses kredensial atau rahasia dalam klaster Kubernetes diinvokasi oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API berhasil diinvokasi oleh pengguna `system:anonymous`. Panggilan API yang dibuat oleh `system:anonymous` tidak diautentikasi. API yang diamati biasanya dikaitkan dengan taktik akses kredenal di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk klaster Kubernetes Anda. Aktivitas ini menunjukkan bahwa akses yang anonim atau tidak diautentikasi diizinkan pada tindakan API yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak terduga, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda disusupi.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada pengguna `system:anonymous` di klaster Anda dan memastikan bahwa semua izin memang diperlukan. Jika izin diberikan secara keliru atau karena niat jahat, Anda harus mencabut akses pengguna dan memulihkan perubahan yang dilakukan

oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS.

Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

CredentialAccess:Kubernetes/TorIPCaller

API yang biasa digunakan untuk mengakses kredensial atau rahasia dalam klaster Kubernetes diinvokasi dari alamat IP simpul keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API diinvokasi dari alamat IP simpul keluar Tor. API yang diamati biasanya dikaitkan dengan taktik akses kredenal di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk klaster Kubernetes Anda. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat mengindikasikan akses yang tidak sah ke sumber daya klaster Kubernetes Anda dengan maksud menyembunyikan identitas penyerang yang sebenarnya.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk menghindari tindakan defensif diinvokasi dari alamat IP berbahaya yang telah diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API diinvokasi dari alamat IP yang terkait dengan aktivitas berbahaya yang telah diketahui. API yang diamati umumnya terkait dengan taktik penghindaran pertahanan di mana penyerang mencoba menyembunyikan tindakan mereka untuk menghindari deteksi.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

API yang biasa digunakan untuk menghindari tindakan defensif diinvokasi dari alamat IP yang disertakan di daftar ancaman kustom.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API diinvokasi dari alamat IP yang disertakan di daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan ini. API yang diamati umumnya terkait dengan taktik penghindaran pertahanan di mana penyerang mencoba menyembunyikan tindakan mereka untuk menghindari deteksi.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan

untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

API yang biasa digunakan untuk menghindari tindakan defensif diinvokasi oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API berhasil diinvokasi oleh pengguna `system:anonymous`. Panggilan API yang dibuat oleh `system:anonymous` tidak diautentikasi. API yang diamati umumnya dikaitkan dengan taktik penghindaran pertahanan di mana penyerang mencoba menyembunyikan tindakan mereka untuk menghindari deteksi. Aktivitas ini menunjukkan bahwa akses yang anonim atau tidak diautentikasi diizinkan pada tindakan API yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak terduga, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda disusupi.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada pengguna `system:anonymous` di klaster Anda dan memastikan bahwa semua izin memang diperlukan. Jika izin diberikan secara keliru atau karena niat jahat, Anda harus mencabut akses pengguna dan memulihkan perubahan yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS.

Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

DefenseEvasion:Kubernetes/TorIPCaller

API yang biasa digunakan untuk menghindari tindakan defensif diinvokasi dari alamat IP simpul keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API diinvokasi dari alamat IP simpul keluar Tor. API yang diamati umumnya terkait dengan taktik penghindaran pertahanan di mana penyerang mencoba menyembunyikan tindakan mereka untuk menghindari deteksi. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke klaster Kubernetes Anda dengan maksud menyembunyikan identitas asli musuh.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Discovery:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk menemukan sumber daya di klaster Kubernetes dipanggil dari alamat IP.

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API diinvokasi dari alamat IP yang terkait dengan aktivitas berbahaya yang telah diketahui. API yang diamati biasanya digunakan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah klaster Kubernetes Anda rentan terhadap serangan yang lebih luas.

> **Untuk akses yang tidak diautentikasi**
>
> MaliciousIPCallertemuan tidak dihasilkan untuk akses yang tidak diautentikasi.

SuccessfulAnonymousAccessTemuan dihasilkan untuk akses yang tidak diautentikasi atau anonim.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Discovery:Kubernetes/MaliciousIPCaller.Custom

API yang biasa digunakan untuk menemukan sumber daya dalam klaster Kubernetes diinvokasi dari alamat IP yang disertakan di daftar ancaman kustom.

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API diinvokasi dari alamat IP yang disertakan di daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan ini. API yang diamati biasanya digunakan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah klaster Kubernetes Anda rentan terhadap serangan yang lebih luas.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan

oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Discovery:Kubernetes/SuccessfulAnonymousAccess

API yang biasa digunakan untuk menemukan sumber daya dalam klaster Kubernetes diinvokasi oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API berhasil diinvokasi oleh pengguna `system:anonymous`. Panggilan API yang dibuat oleh `system:anonymous` tidak diautentikasi. API yang diamati umumnya terkait dengan tahap penemuan serangan ketika penyerang mengumpulkan informasi tentang klaster Kubernetes Anda. Aktivitas ini menunjukkan bahwa akses yang anonim atau tidak diautentikasi diizinkan pada tindakan API yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak terduga, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda disusupi.

Jenis temuan ini mengecualikan titik akhir API pemeriksaan kesehatan seperti`/healthz`,, `/livez/readyz`, dan. `/version`

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada pengguna `system:anonymous` di klaster Anda dan memastikan bahwa semua izin memang diperlukan. Jika izin diberikan secara keliru atau karena niat jahat, Anda harus mencabut akses pengguna dan memulihkan perubahan yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS.

Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Discovery:Kubernetes/TorIPCaller

API yang biasa digunakan untuk menemukan sumber daya dalam klaster Kubernetes diinvokasi dari alamat IP simpul keluar Tor.

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API diinvokasi dari alamat IP simpul keluar Tor. API yang diamati biasanya digunakan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah klaster Kubernetes Anda rentan terhadap serangan yang lebih luas. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke klaster Kubernetes Anda dengan maksud menyembunyikan identitas asli musuh.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *`KubernetesUserDetails`* bagian ini adalah*`system:anonymous`*, selidiki mengapa pengguna anonim diizinkan untuk memanggil APIDan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Execution:Kubernetes/ExecInKubeSystemPod

Sebuah perintah dijalankan di dalam sebuah pod di dalam namespace **`kube-system`**

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa sebuah perintah telah dijalankan di sebuah pod di dalam `kube-system` namespace menggunakan Kubernetes exec API. `kube-system`namespace adalah ruang nama default, yang terutama digunakan untuk komponen tingkat sistem seperti dan. `kube-dns` `kube-proxy` Sangat jarang untuk mengeksekusi perintah di dalam pod atau kontainer di bawah `kube-system` namespace dan mungkin menunjukkan aktivitas yang mencurigakan.

Rekomendasi remediasi:

Jika eksekusi perintah ini tidak terduga, kredensial identitas pengguna yang digunakan untuk menjalankan perintah mungkin disusupi. Cabut akses pengguna dan pulihkan perubahan yang

dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Impact:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk mengutak-atik sumber daya dalam klaster Kubernetes diinvokasi dari alamat IP berbahaya yang telah diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API diinvokasi dari alamat IP yang terkait dengan aktivitas berbahaya yang telah diketahui. API yang diamati umumnya dikaitkan dengan taktik dampak di mana musuh mencoba memanipulasi, mengganggu, atau menghancurkan data dalam lingkungan Anda. AWS

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Impact:Kubernetes/MaliciousIPCaller.Custom

API yang biasa digunakan untuk mengutak-atik sumber daya dalam klaster Kubernetes diinvokasi dari alamat IP yang disertakan di daftar ancaman kustom.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API diinvokasi dari alamat IP yang disertakan di daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian

Informasi Tambahan dari detail temuan ini. API yang diamati umumnya dikaitkan dengan taktik dampak di mana musuh mencoba memanipulasi, mengganggu, atau menghancurkan data dalam lingkungan Anda. AWS

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Impact:Kubernetes/SuccessfulAnonymousAccess

API yang biasa digunakan untuk mengutak-atik sumber daya dalam klaster Kubernetes diinvokasi oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API berhasil diinvokasi oleh pengguna `system:anonymous`. Panggilan API yang dibuat oleh `system:anonymous` tidak diautentikasi. API yang diamati umumnya terkait dengan tahap dampak serangan ketika penyerang mengganggu sumber daya di klaster Anda. Aktivitas ini menunjukkan bahwa akses yang anonim atau tidak diautentikasi diizinkan pada tindakan API yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak terduga, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda disusupi.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada pengguna `system:anonymous` di klaster Anda dan memastikan bahwa semua izin memang diperlukan. Jika izin diberikan secara keliru atau karena niat jahat, Anda harus mencabut akses pengguna dan memulihkan perubahan yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS.

Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Impact:Kubernetes/TorIPCaller

API yang biasa digunakan untuk mengutak-atik sumber daya dalam klaster Kubernetes diinvokasi dari alamat IP simpul keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API diinvokasi dari alamat IP simpul keluar Tor. API yang diamati umumnya terkait dengan taktik dampak di mana penyerang mencoba memanipulasi, mengganggu, atau menghancurkan data dalam lingkungan AWS Anda. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke klaster Kubernetes Anda dengan maksud menyembunyikan identitas asli musuh.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Persistence:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk mendapatkan akses persisten ke klaster Kubernetes diinvokasi dari alamat IP berbahaya yang telah diketahui.

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API diinvokasi dari alamat IP yang terkait dengan aktivitas berbahaya yang telah diketahui. API yang diamati umumnya terkait dengan taktik persisten di mana penyerang telah mendapatkan akses ke klaster Kubernetes Anda dan mencoba mempertahankan akses tersebut.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Persistence:Kubernetes/MaliciousIPCaller.Custom

API yang biasa digunakan untuk mendapatkan akses persisten ke klaster Kubernetes diinvokasi dari alamat IP yang disertakan di daftar ancaman kustom.

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API diinvokasi dari alamat IP yang disertakan di daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan ini. API yang diamati umumnya terkait dengan taktik persisten di mana penyerang telah mendapatkan akses ke klaster Kubernetes Anda dan mencoba mempertahankan akses tersebut.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas

tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Persistence:Kubernetes/SuccessfulAnonymousAccess

API yang biasa digunakan untuk mendapatkan izin tingkat tinggi ke klaster Kubernetes diinvokasi oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API berhasil diinvokasi oleh pengguna `system:anonymous`. Panggilan API yang dibuat oleh `system:anonymous` tidak diautentikasi. API yang diamati umumnya terkait dengan taktik persisten di mana penyerang telah mendapatkan akses ke klaster Anda dan mencoba mempertahankan akses tersebut. Aktivitas ini menunjukkan bahwa akses yang anonim atau tidak diautentikasi diizinkan pada tindakan API yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak terduga, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda disusupi.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada pengguna `system:anonymous` di klaster Anda dan memastikan bahwa semua izin memang diperlukan. Jika izin diberikan secara keliru atau karena niat jahat, Anda harus mencabut akses pengguna dan memulihkan perubahan yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS.

Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Persistence:Kubernetes/TorIPCaller

API yang biasa digunakan untuk mendapatkan akses persisten ke klaster Kubernetes diinvokasi dari alamat IP simpul keluar Tor.

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API diinvokasi dari alamat IP simpul keluar Tor. API yang diamati umumnya terkait dengan taktik persisten di mana penyerang telah mendapatkan akses ke klaster Kubernetes Anda dan mencoba mempertahankan akses tersebut. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Simpul Tor terakhir disebut sebagai simpul keluar. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah bagian `KubernetesUserDetails` adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk menginvokasi API dan mencabut izin, jika diperlukan, dengan mengikuti instruksi dalam Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas tersebut berbahaya, cabut akses pengguna dan pulihkan perubahan apa pun yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Akun layanan default diberi hak akses admin pada klaster Kubernetes.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa akun layanan default untuk sebuah namespace di klaster Kubernetes Anda diberi hak akses admin. Kubernetes membuat akun layanan default untuk semua namespace di klaster. Layanan ini secara otomatis menetapkan akun layanan default sebagai identitas ke pod yang belum dikaitkan secara eksplisit ke akun layanan lain. Jika akun layanan default memiliki hak akses admin, maka pod dapat diluncurkan secara tidak sengaja dengan hak akses admin. Jika perilaku ini tidak terduga, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda disusupi.

Rekomendasi remediasi:

Anda tidak boleh menggunakan akun layanan default untuk memberikan izin kepada pod. Sebagai gantinya, Anda harus membuat akun layanan khusus untuk setiap beban kerja dan memberikan

izin ke akun tersebut berdasarkan kebutuhan. Untuk mengatasi masalah ini, Anda harus membuat akun layanan khusus untuk semua pod dan beban kerja Anda dan memperbarui pod dan beban kerja untuk bermigrasi dari akun layanan default ke akun khususnya. Maka Anda harus menghapus izin admin dari akun layanan default. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Policy:Kubernetes/AnonymousAccessGranted

Pengguna **`system:anonymous`** diberikan izin API pada klaster Kubernetes.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa pengguna di klaster Kubernetes Anda berhasil membuat `ClusterRoleBinding` atau `RoleBinding` untuk mengikat pengguna `system:anonymous` ke sebuah peran. Hal ini memungkinkan akses yang tidak diautentikasi ke operasi API yang diizinkan oleh peran. Jika perilaku ini tidak terduga, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda disusupi.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada pengguna `system:anonymous` atau grup `system:unauthenticated` di klaster Anda dan mencabut akses anonim yang tidak perlu. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS. Jika izin diberikan karena niat jahat, Anda harus mencabut akses pengguna yang memberikan izin dan memulihkan perubahan yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Policy:Kubernetes/ExposedDashboard

Dasbor untuk klaster Kubernetes diekspos ke internet

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa dasbor Kubernetes untuk klaster Anda diekspos ke internet melalui layanan Penyeimbang Beban. Dasbor yang terekspos akan membuat antarmuka manajemen

klaster Anda dapat diakses dari internet dan memungkinkan penyerang mengeksploitasi celah kontrol autentikasi dan akses yang mungkin ada.

Rekomendasi remediasi:

Anda harus memastikan bahwa otentikasi dan otorisasi yang kuat diberlakukan di Dasbor Kubernetes. Anda juga harus menerapkan kontrol akses jaringan untuk membatasi akses ke dasbor dari alamat IP tertentu.

Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Policy:Kubernetes/KubeflowDashboardExposed

Bagian Kubeflow dasbor untuk cluster Kubernetes diekspos ke Internet

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa dasbor Kubeflow untuk klaster Anda diekspos ke Internet oleh layanan Load Balancer. Dasbor Kubeflow yang terbuka membuat antarmuka manajemen lingkungan Kubeflow Anda dapat diakses dari Internet dan memungkinkan musuh untuk mengeksploitasi celah otentikasi dan kontrol akses apa pun yang mungkin ada.

Rekomendasi remediasi:

Anda harus memastikan bahwa otentikasi dan otorisasi yang kuat diberlakukan di Dasbor Kubeflow. Anda juga harus menerapkan kontrol akses jaringan untuk membatasi akses ke dasbor dari alamat IP tertentu.

Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

API Kubernetes yang biasa digunakan untuk mengakses rahasia dipanggil dengan cara yang anomali.

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API beranomali untuk mengambil rahasia klaster sensitif diinvokasi oleh pengguna Kubernetes di klaster Anda. API yang diamati biasanya dikaitkan dengan taktik akses kredensial yang dapat mengakibatkan eskalasi berhak akses dan akses lebih lanjut dalam klaster Anda. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau AWS kredenal Anda dikompromikan.

API yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas API pengguna dalam kluster EKS Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML melacak beberapa faktor operasi API seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang diberikan kepada pengguna Kubernetes di klaster Anda dan pastikan bahwa semua izin ini diperlukan. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Jika AWS kredensialnya dikompromikan, lihat. Memperbaiki potensi terganggu AWS credentials

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Sebuah RoleBinding atau ClusterRoleBinding ke peran yang terlalu permisif atau namespace yang sensitif telah dibuat atau dimodifikasi di klaster Kubernetes Anda.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika RoleBinding atau ClusterRoleBinding melibatkan ClusterRoles `admin` atau`cluster-admin`, tingkat keparahannya Tinggi.

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa pengguna di klaster Kubernetes Anda membuat `RoleBinding` atau `ClusterRoleBinding` untuk mengikat pengguna ke peran dengan izin admin atau ruang nama sensitif. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau AWS kredenal Anda dikompromikan.

API yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas API pengguna dalam kluster EKS Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang diberikan kepada pengguna Kubernetes. Izin ini didefinisikan dalam peran dan subjek yang terlibat dalam `RoleBinding` dan`ClusterRoleBinding`. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Jika AWS kredensialnya dikompromikan, lihat. Memperbaiki potensi terganggu AWS credentials

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Sebuah perintah dieksekusi di dalam pod dengan cara yang anomali.

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa perintah dijalankan di pod menggunakan API exec Kubernetes. Exec API Kubernetes memungkinkan menjalankan perintah arbitrer dalam sebuah pod. Jika perilaku ini tidak diharapkan untuk pengguna, namespace, atau pod, ini mungkin menunjukkan kesalahan konfigurasi atau AWS kredensialmu disusupi.

API yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas API pengguna dalam kluster EKS Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan

oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Jika eksekusi perintah ini tidak terduga, kredensi identitas pengguna yang digunakan untuk menjalankan perintah mungkin telah dikompromikan. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Jika AWS kredensialnya dikompromikan, lihat. Memperbaiki potensi terganggu AWS credentials

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Beban kerja diluncurkan dengan wadah istimewa dengan cara yang anomali.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa beban kerja diluncurkan dengan wadah istimewa di klaster Amazon EKS Anda. Sebuah kontainer berhak akses memiliki akses tingkat root ke host. Pengguna yang tidak sah dapat meluncurkan kontainer berhak akses sebagai taktik eskalasi hak akses untuk terlebih dahulu mendapatkan akses ke host kemudian menyusupinya.

Pembuatan atau modifikasi wadah yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API pengguna dan aktivitas image container dalam kluster EKS Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensi identitas pengguna yang digunakan untuk meluncurkan penampung mungkin telah disusupi. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Jika AWS kredensialnya dikompromikan, lihat. Memperbaiki potensi terganggu AWS credentials

Jika peluncuran kontainer ini diharapkan, Anda disarankan untuk menggunakan aturan penekanan dengan kriteria filter berdasarkan `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` bidang. Dalam kriteria filter, `imagePrefix` bidang harus memiliki nilai yang sama dengan `imagePrefix` bidang yang ditentukan dalam temuan. Untuk informasi selengkapnya, lihat Aturan penindasan di GuardDuty.

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount

Beban kerja diterapkan dengan cara yang anomali, dengan jalur host sensitif dipasang di dalam beban kerja.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa beban kerja diluncurkan dengan kontainer yang disertai jalur host sensitif di bagian `volumeMounts`. Hal ini berpotensi membuat jalur host sensitif dapat diakses dan ditulis dari dalam kontainer. Teknik ini biasanya digunakan oleh pengguna yang tidak sah untuk mendapatkan akses ke sistem file host.

Pembuatan atau modifikasi wadah yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API pengguna dan aktivitas image container dalam kluster EKS Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensi identitas pengguna yang digunakan untuk meluncurkan penampung mungkin telah disusupi. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Jika AWS kredensialnya dikompromikan, lihat. Memperbaiki potensi terganggu AWS credentials

Jika peluncuran kontainer ini diharapkan, Anda disarankan untuk menggunakan aturan penekanan dengan kriteria filter berdasarkan `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` bidang. Dalam kriteria filter, `imagePrefix` bidang harus memiliki nilai yang sama dengan `imagePrefix` bidang yang ditentukan dalam temuan. Untuk informasi selengkapnya, lihat Aturan penindasan di GuardDuty.

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Beban kerja diluncurkan dengan cara yang anomali.

Tingkat keparahan default: Rendah*

> **Note**
>
> Tingkat keparahan default adalah Rendah. Namun, jika beban kerja berisi nama gambar yang berpotensi mencurigakan, seperti alat pentest yang dikenal, atau wadah yang menjalankan perintah yang berpotensi mencurigakan saat peluncuran, seperti perintah shell terbalik, maka tingkat keparahan jenis temuan ini akan dianggap sebagai Medium.

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa beban kerja Kubernetes dibuat atau dimodifikasi secara anomali, seperti aktivitas API, image container baru, atau konfigurasi beban kerja berisiko, di dalam klaster Amazon EKS Anda. Pengguna yang tidak sah dapat meluncurkan kontainer sebagai taktik untuk melaksanakan kode arbitrer untuk terlebih dahulu mendapatkan akses ke host kemudian membahayakannya.

Pembuatan atau modifikasi wadah yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API pengguna

dan aktivitas image container dalam kluster EKS Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensi identitas pengguna yang digunakan untuk meluncurkan penampung mungkin telah disusupi. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Jika AWS kredensialnya dikompromikan, lihat. Memperbaiki potensi terganggu AWS credentials

Jika peluncuran kontainer ini diharapkan, Anda disarankan untuk menggunakan aturan penekanan dengan kriteria filter berdasarkan `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` bidang. Dalam kriteria filter, `imagePrefix` bidang harus memiliki nilai yang sama dengan `imagePrefix` bidang yang ditentukan dalam temuan. Untuk informasi selengkapnya, lihat Aturan penindasan di GuardDuty.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Peran yang sangat permisif atau ClusterRole diciptakan atau dimodifikasi dengan cara yang anomali.

Tingkat keparahan default: Rendah

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API anomali untuk membuat `Role` atau `ClusterRole` dengan izin berlebihan dipanggil oleh pengguna Kubernetes di cluster Amazon EKS Anda. Aktor dapat menggunakan pembuatan peran dengan izin yang kuat untuk menghindari penggunaan peran mirip admin bawaan dan menghindari deteksi. Izin yang berlebihan dapat menyebabkan eskalasi istimewa, eksekusi kode jarak jauh, dan berpotensi mengontrol namespace atau cluster. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredenal Anda dikompromikan.

API yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas API pengguna dalam klaster Amazon EKS Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang ditentukan dalam `Role` atau `ClusterRole` untuk memastikan bahwa semua izin diperlukan dan ikuti prinsip hak istimewa paling sedikit. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Jika AWS kredensialnya dikompromikan, lihat. Memperbaiki potensi terganggu AWS credentials

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Seorang pengguna memeriksa izin akses mereka dengan cara yang tidak wajar.

Tingkat keparahan default: Rendah

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa pengguna di klaster Kubernetes Anda berhasil memeriksa apakah izin kuat yang diketahui yang dapat menyebabkan eskalasi istimewa dan eksekusi kode jarak jauh, diizinkan atau tidak. Misalnya, perintah umum yang digunakan untuk memeriksa izin untuk pengguna adalah `kubectl auth can-i`. Jika perilaku ini tidak terduga, ini mungkin menunjukkan kesalahan konfigurasi atau keamanan kredensial Anda telah dilanggar.

API yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas API pengguna dalam klaster Amazon EKS Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, izin diperiksa, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang diberikan kepada pengguna Kubernetes untuk memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Jika AWS kredensialnya dikompromikan, lihat. Memperbaiki potensi terganggu AWS credentials

GuardDuty Jenis penemuan Runtime Monitoring

Amazon GuardDuty menghasilkan temuan Runtime Monitoring berikut untuk menunjukkan potensi ancaman berdasarkan perilaku tingkat sistem operasi dari host dan container Amazon EC2 di cluster Amazon EKS, beban kerja Fargate dan Amazon ECS, serta instans Amazon EC2.

GuardDuty menghasilkan beberapa jenis pencarian Runtime Monitoring hanya jika Anda mengaktifkan Aturan Deteksi Kustom untuk Pemantauan Runtime. Untuk jenis temuan ini, lihatMenemukan jenis yang memerlukan Aturan Deteksi Kustom.

> **Note**
>
> Jenis pencarian Runtime Monitoring didasarkan pada log runtime yang dikumpulkan dari host. Log berisi bidang seperti jalur file yang dapat dikontrol oleh aktor jahat. Bidang ini juga termasuk dalam GuardDuty temuan untuk memberikan konteks runtime. Saat memproses temuan Runtime Monitoring di luar GuardDuty konsol, Anda harus membersihkan bidang pencarian. Misalnya, Anda dapat menyandikan HTML bidang pencarian saat menampilkannya di halaman web.

Topik

- Menemukan tipe yang dihasilkan Runtime Monitoring secara default
- Menemukan jenis yang memerlukan Aturan Deteksi Kustom

Menemukan tipe yang dihasilkan Runtime Monitoring secara default

GuardDuty menghasilkan jenis temuan di bagian ini saat Anda mengaktifkan Runtime Monitoring. Anda tidak perlu mengaktifkan Aturan Deteksi Kustom untuk Pemantauan Waktu Proses untuk mendapatkan jenis temuan ini.

Topik

- CryptoCurrency:Runtime/BitcoinTool.B
- Backdoor:Runtime/C&CActivity.B
- UnauthorizedAccess:Runtime/TorRelay
- UnauthorizedAccess:Runtime/TorClient
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/DropPoint
- CryptoCurrency:Runtime/BitcoinTool.B! DNS
- Backdoor:Runtime/C&CActivity.B! DNS
- Trojan:Runtime/BlackholeTraffic! DNS
- Trojan:Runtime/DropPoint! DNS
- Trojan:Runtime/DGADomainRequest.C! DNS
- Trojan:Runtime/DriveBySourceTraffic! DNS
- Trojan:Runtime/PhishingDomainRequest! DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- UnauthorizedAccess:Runtime/MetadataDNSRebind
- Execution:Runtime/NewBinaryExecuted
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- DefenseEvasion:Runtime/ProcessInjection.Proc
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- DefenseEvasion:Runtime/FilelessExecution

- Impact:Runtime/CryptoMinerExecuted
- Execution:Runtime/NewLibraryLoaded
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Execution:Runtime/SuspiciousTool
- Execution:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted
- Execution:Runtime/MaliciousFileExecuted.Custom
- Execution:Runtime/SuspiciousShellCreated
- PrivilegeEscalation:Runtime/ElevationToRoot
- Discovery:Runtime/SuspiciousCommand
- Persistence:Runtime/SuspiciousCommand
- PrivilegeEscalation:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/KernelModuleLoaded
- Persistence:Runtime/SensitiveFileModified
- PrivilegeEscalation:Runtime/SensitiveFileModified
- DefenseEvasion:Runtime/SensitiveFileModified

CryptoCurrency:Runtime/BitcoinTool.B

Instans Amazon EC2 atau sebuah kontainer mengkueri alamat IP yang berhubungan dengan aktivitas terkait mata uang kripto.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda sedang menanyakan alamat IP yang terkait dengan aktivitas terkait

cryptocurrency. Pelaku ancaman dapat berusaha mengambil kendali atas sumber daya komputasi guna memanfaatkannya dengan tujuan jahat untuk penambangan mata uang kripto yang tidak sah.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika Anda menggunakan instans EC2 ini atau sebuah kontainer untuk menambang atau mengelola mata uang kripto, atau salah satunya berkaitan dengan aktivitas blockchain, temuan CryptoCurrency:Runtime/BitcoinTool.B dapat merepresentasikan aktivitas yang memang diduga untuk lingkungan Anda. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria filter pertama harus menggunakan atribut Jenis temuan dengan nilai `CryptoCurrency:Runtime/BitcoinTool.B`. Kriteria filter kedua harus berupa ID instans untuk instans atau ID Citra Kontainer untuk kontainer yang digunakan dalam aktivitas terkait mata uang kripto atau blockchain. Untuk informasi lebih lanjut, lihat Aturan penekanan.

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Backdoor:Runtime/C&CActivity.B

Instans Amazon EC2 atau wadah menanyakan IP yang terkait dengan server perintah dan kontrol yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah dalam AWS lingkungan Anda menanyakan alamat IP yang terkait dengan server perintah dan kontrol (C&C) yang diketahui. Instans yang tercantum atau kontainer mungkin berpotensi disusupi. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin mencakup PC, server, perangkat seluler, dan perangkat Internet untuk Segala, yang terinfeksi dan dikendalikan oleh sebuah jenis malware yang sama. Botnet sering digunakan untuk mendistribusikan malware dan

mengumpulkan informasi yang disusupi, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet tersebut, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan Penolakan Layanan Terdistribusi (DDoS).

> **Note**
>
> Jika IP yang dikueri terkait dengan log4j, bidang temuan terkait akan berisi nilai berikut:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

UnauthorizedAccess:Runtime/TorRelay

Instans Amazon EC2 Anda atau sebuah kontainer membuat koneksi ke jaringan Tor sebagai relai Tor.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda membuat koneksi ke jaringan Tor dengan cara yang menunjukkan bahwa itu bertindak sebagai relai Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Tor meningkatkan anonimitas komunikasi dengan meneruskan lalu lintas klien yang kemungkinan terlarang dari satu relai Tor ke relai lainnya.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel

temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

UnauthorizedAccess:Runtime/TorClient

Instans Amazon EC2 Anda atau sebuah kontainer membuat koneksi ke simpul Tor Guard atau simpul Authority.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda membuat koneksi ke Tor Guard atau node Authority. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Simpul Tor Guard dan Authority bertindak sebagai gateway awal ke dalam jaringan Tor. Lalu lintas ini dapat menunjukkan bahwa instans EC2 atau sebuah kontainer ini berpotensi disusupi dan bertindak sebagai klien di jaringan Tor. Temuan ini mungkin menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Trojan:Runtime/BlackholeTraffic

Instans Amazon EC2 atau sebuah kontainer mencoba berkomunikasi dengan alamat IP host jarak jauh yang merupakan black hole yang telah diketahui.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda mungkin terganggu karena mencoba berkomunikasi dengan alamat IP lubang hitam (atau lubang wastafel). Black hole adalah tempat di jaringan di mana lalu lintas yang masuk atau keluar diam-diam dibuang tanpa menginformasikan sumber bahwa datanya tidak sampai ke penerima yang dimaksudkan. Alamat IP black hole menentukan mesin host yang tidak berjalan atau alamat yang tidak memiliki host yang ditetapkan.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Trojan:Runtime/DropPoint

Instans Amazon EC2 atau sebuah kontainer mencoba berkomunikasi dengan alamat IP host jarak jauh yang telah diketahui menyimpan kredensial dan data curian lainnya yang diambil oleh malware.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda mencoba berkomunikasi dengan alamat IP host jarak jauh yang diketahui menyimpan kredensyal dan data curian lainnya yang ditangkap oleh malware.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

CryptoCurrency:Runtime/BitcoinTool.B! DNS

Instans Amazon EC2 atau sebuah kontainer mengkueri nama domain yang terkait dengan aktivitas mata uang kripto.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda sedang menanyakan nama domain yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Pelaku ancaman dapat berusaha mengambil kendali atas sumber daya komputasi guna memanfaatkannya dengan tujuan jahat untuk penambangan mata uang kripto yang tidak sah.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika Anda menggunakan instans atau wadah EC2 ini untuk menambang atau mengelola cryptocurrency, atau salah satu dari ini terlibat dalam aktivitas blockchain, CryptoCurrency:Runtime/BitcoinTool.B!DNS temuan ini bisa menjadi aktivitas yang diharapkan untuk lingkungan Anda. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. Kriteria filter kedua harus berupa ID Instance dari instance atau Container Image ID dari container yang terlibat dalam aktivitas cryptocurrency atau blockchain. Untuk informasi selengkapnya, lihat Aturan Penindasan.

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Backdoor:Runtime/C&CActivity.B! DNS

Instans Amazon EC2 atau sebuah kontainer mengkueri nama domain yang terkait dengan server perintah dan kontrol yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah dalam AWS lingkungan Anda sedang menanyakan nama domain yang terkait dengan server perintah dan kontrol (C&C) yang diketahui. Instans EC2 yang tercantum atau kontainer mungkin disusupi. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin termasuk PC, server, perangkat seluler, dan perangkat Internet untuk Segala, yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disusupi, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet tersebut, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan Penolakan Layanan Terdistribusi (DDoS).

> **Note**
>
> Jika nama domain yang dikueri terkait dengan log4j, bidang temuan terkait akan berisi nilai berikut:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> Untuk menguji bagaimana GuardDuty menghasilkan jenis temuan ini, Anda dapat membuat permintaan DNS dari instance Anda (menggunakan `dig` untuk Linux atau `nslookup` untuk Windows) terhadap domain `guarddutyc2activityb.com` pengujian.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Trojan:Runtime/BlackholeTraffic! DNS

Instans Amazon EC2 atau sebuah kontainer mengkueri nama domain yang diarahkan ke alamat IP black hole.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda mungkin terganggu karena menanyakan nama domain yang sedang dialihkan ke alamat IP lubang hitam. Black hole adalah tempat di jaringan di mana lalu lintas yang masuk atau keluar diam-diam dibuang tanpa menginformasikan sumber bahwa datanya tidak sampai ke penerima yang dimaksudkan.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Trojan:Runtime/DropPoint! DNS

Instans Amazon EC2 atau sebuah kontainer mengkueri nama domain host jarak jauh yang telah diketahui menyimpan kredensial dan data curian lainnya yang diambil oleh malware.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda menanyakan nama domain host jarak jauh yang diketahui menyimpan kredensyal dan data curian lainnya yang ditangkap oleh malware.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Trojan:Runtime/DGADomainRequest.C! DNS

Instans Amazon EC2 atau sebuah kontainer mengkueri pada domain yang dihasilkan secara algoritmik. Domain tersebut biasanya digunakan oleh malware dan bisa menjadi indikasi dari instans EC2 atau sebuah kontainer yang disusupi.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda mencoba menanyakan domain algoritma pembuatan domain (DGA). Sumber daya Anda mungkin telah disusupi.

DGA digunakan untuk secara berkala menghasilkan sejumlah besar nama domain yang dapat digunakan sebagai titik pertemuan dengan server perintah dan kontrol (C&C)-nya. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah kepada anggota botnet, yang merupakan kumpulan perangkat yang terhubung ke internet yang terinfeksi dan dikendalikan oleh jenis malware yang sama. Banyaknya potensi titik pertemuan mempersulit untuk mematikan botnet secara efektif karena komputer yang terinfeksi mencoba menghubungi beberapa nama domain ini setiap hari untuk menerima pembaruan atau perintah.

> **Note**
>
> Temuan ini didasarkan pada domain DGA yang diketahui dari umpan intelijen GuardDuty ancaman.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Trojan:Runtime/DriveBySourceTraffic! DNS

Instans Amazon EC2 atau wadah menanyakan nama domain host jarak jauh yang merupakan sumber serangan unduhan yang diketahui. Drive-By

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda mungkin terganggu karena menanyakan nama domain host jarak jauh yang merupakan sumber serangan unduhan drive-by yang diketahui. Hal ini adalah pengunduhan perangkat lunak komputer yang tidak diinginkan dari internet yang dapat memicu penginstalan virus, spyware, atau malware secara otomatis.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Trojan:Runtime/PhishingDomainRequest! DNS

Instans Amazon EC2 atau sebuah kontainer mengkueri pada domain yang digunakan dalam serangan phishing.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda mencoba menanyakan domain yang terlibat dalam serangan phishing. Domain phishing dibuat oleh seseorang yang berpura-pura sebagai lembaga resmi untuk membujuk individu memberikan data sensitif, seperti informasi pengenal pribadi, detail perbankan dan kartu kredit, serta kata sandi. Instans EC2 Anda atau kontainer mungkin mencoba mengambil data sensitif yang disimpan di situs web phishing, atau mungkin mencoba menyiapkan situs web phishing. Instans EC2 Anda atau kontainer mungkin disusupi.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Impact:Runtime/AbusedDomainRequest.Reputation

Instans Amazon EC2 atau sebuah kontainer mengkueri nama domain bereputasi rendah yang terkait dengan domain yang telah diketahui disusupi.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah dalam AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan domain atau alamat IP yang disalahgunakan yang diketahui. Contoh domain yang disalahgunakan adalah nama domain tingkat atas (TLD) dan nama domain tingkat kedua (2LD)

yang menyediakan pendaftaran subdomain gratis serta penyedia DNS dinamis. Pelaku ancaman cenderung menggunakan layanan ini untuk mendaftarkan domain secara gratis atau dengan biaya rendah. Domain dengan reputasi rendah dalam kategori ini mungkin juga adalah domain kedaluwarsa yang menentukan alamat IP parkir registrar dan oleh karena itu mungkin tidak lagi aktif. IP parkir adalah tempat registrar mengarahkan lalu lintas untuk domain yang belum ditautkan ke layanan apa pun. Instans Amazon EC2 yang tercantum atau kontainer dapat disusupi karena pelaku ancaman umumnya menggunakan registrar atau layanan ini untuk C&C dan distribusi malware.

Domain bereputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberikan peringkat untuk karakteristik domain guna menentukan kemungkinan bahwa domain tersebut berbahaya.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Impact:Runtime/BitcoinDomainRequest.Reputation

Sebuah instans Amazon EC2 atau sebuah kontainer mengkueri nama domain bereputasi rendah yang berhubungan dengan aktivitas terkait mata uang kripto.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Pelaku ancaman dapat berusaha mengambil kendali atas sumber daya komputasi guna memanfaatkannya dengan tujuan jahat untuk penambangan mata uang kripto yang tidak sah.

Domain bereputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberikan peringkat untuk karakteristik domain guna menentukan kemungkinan bahwa domain tersebut berbahaya.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika Anda menggunakan instans EC2 ini atau wadah untuk menambang atau mengelola cryptocurrency, atau jika sumber daya ini terlibat dalam aktivitas blockchain, temuan ini dapat mewakili aktivitas yang diharapkan untuk lingkungan Anda. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria filter pertama harus menggunakan atribut Jenis temuan dengan nilai `Impact:Runtime/BitcoinDomainRequest.Reputation`. Kriteria filter kedua harus berupa ID Instance dari instance atau ID Gambar Kontainer dari container terlibat dalam aktivitas terkait cryptocurrency atau blockchain. Untuk informasi selengkapnya, lihat Aturan penindasan.

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Impact:Runtime/MaliciousDomainRequest.Reputation

Instans Amazon EC2 atau sebuah kontainer mengkueri domain bereputasi rendah yang terkait dengan domain berbahaya yang telah diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan domain berbahaya atau alamat IP yang diketahui. Misalnya, domain dapat dikaitkan dengan alamat IP sinkhole yang diketahui. Domain sinkhole adalah domain yang sebelumnya dikendalikan oleh pelaku ancaman, dan permintaan yang dibuat untuk domain tersebut dapat menunjukkan bahwa instans disusupi. Domain ini juga dapat dikorelasikan dengan kampanye berbahaya atau algoritma pembuatan domain yang diketahui.

Domain bereputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberikan peringkat untuk karakteristik domain guna menentukan kemungkinan bahwa domain tersebut berbahaya.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Instans Amazon EC2 atau sebuah kontainer mengkueri nama domain bereputasi rendah yang bersifat mencurigakan karena umurnya, atau popularitas yang rendah.

Tingkat keparahan default: Rendah

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah dalam AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang diduga berbahaya. Karakteristik yang diamati dari domain ini konsisten dengan domain berbahaya yang diamati sebelumnya. Namun, model reputasi kami tidak dapat secara definitif menghubungkannya dengan ancaman yang diketahui. Domain-domain ini biasanya baru diamati atau menerima jumlah lalu lintas yang rendah.

Domain bereputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberikan peringkat untuk karakteristik domain guna menentukan kemungkinan bahwa domain tersebut berbahaya.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Instans Amazon EC2 atau sebuah kontainer melakukan pencarian DNS yang di-resolve menjadi layanan metadata instans.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

> **Note**
>
> Saat ini, tipe temuan ini hanya didukung untuk arsitektur AMD64.

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans EC2 yang terdaftar atau wadah di AWS lingkungan Anda sedang menanyakan domain yang menyelesaikan ke alamat IP metadata EC2 (169.254.169.254). Kueri DNS semacam ini dapat mengindikasikan bahwa instans adalah target dari teknik rebinding DNS. Teknik ini dapat digunakan untuk mendapatkan metadata dari instans EC2, termasuk kredensial IAM yang terkait dengan instans.

Rebinding DNS adalah proses yang menipu sebuah aplikasi yang berjalan di instans EC2 untuk memuat data pengembalian dari URL, dengan nama domain di URL tersebut di-resolve menjadi alamat IP metadata EC2 (`169.254.169.254`). Hal ini menyebabkan aplikasi mengakses metadata EC2 dan mungkin membuatnya dapat diakses penyerang.

Metadata EC2 dapat diakses menggunakan rebinding DNS hanya jika instans EC2 menjalankan aplikasi rentan yang memungkinkan injeksi URL, atau jika seseorang mengakses URL di browser web yang berjalan pada instans EC2.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Menanggapi temuan ini, Anda harus mengevaluasi jika ada aplikasi rentan yang berjalan di instans EC2 atau kontainer, atau jika seseorang menggunakan browser untuk mengakses domain yang diidentifikasi dalam temuan. Jika akar penyebabnya adalah aplikasi yang rentan, perbaiki kerentanan

tersebut. Jika seseorang mengakses domain yang teridentifikasi melalui browser, blokir domain tersebut atau cegah pengguna mengaksesnya. Jika Anda melihat temuan ini terkait dengan kedua kasus di atas, Anda harus Mencabut sesi yang terkait dengan instans EC2.

Beberapa AWS pelanggan sengaja memetakan alamat IP metadata ke nama domain di server DNS otoritatif mereka. Jika penggunaan lingkungan Anda memang demikian adanya, kami menyarankan Anda mengatur aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria filter pertama harus menggunakan atribut Jenis temuan dengan nilai `UnauthorizedAccess:Runtime/MetadataDNSRebind`. Kriteria filter kedua harus domain permintaan DNS atau ID Gambar Kontainer wadah. Nilai domain permintaan DNS harus sesuai dengan domain yang telah Anda petakan ke alamat IP metadata (). `169.254.169.254` Untuk informasi tentang membuat aturan penekanan, lihat Aturan penekanan.

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Execution:Runtime/NewBinaryExecuted

File biner yang baru dibuat atau baru saja dimodifikasi dalam kontainer telah dijalankan.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa file biner yang baru dibuat atau yang baru saja dimodifikasi, dalam wadah telah dieksekusi. Praktik terbaiknya adalah menjaga kontainer tetap bersifat imutabel pada saat runtime, dan file biner, skrip, atau pustaka tidak boleh dibuat atau dimodifikasi selama masa pakai kontainer. Perilaku ini menunjukkan bahwa pelaku berbahaya yang telah mendapatkan akses ke kontainer telah mengunduh dan menjalankan malware atau perangkat lunak lain sebagai bagian dari penyusupan yang potensial. Meskipun jenis aktivitas ini bisa menjadi indikasi adanya penyusupan, ini juga merupakan pola penggunaan yang umum. Oleh karena itu, GuardDuty gunakan mekanisme untuk mengidentifikasi contoh mencurigakan dari aktivitas ini dan menghasilkan jenis temuan ini hanya untuk contoh yang mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Untuk mengidentifikasi proses modifikasi dan biner baru, lihat detail proses Modifikasi dan detail Proses

Rincian proses modifikasi termasuk dalam `service.runtimeDetails.context.modifyingProcess` bidang penemuan JSON, atau di bawah Proses Memodifikasi di panel rincian temuan. Untuk jenis temuan ini, proses modifikasi adalah`/usr/bin/dpkg`, seperti yang diidentifikasi oleh `service.runtimeDetails.context.modifyingProcess.executablePath` bidang temuan JSON, atau sebagai bagian dari Proses Memodifikasi di panel rincian temuan.

Rincian biner baru atau modifikasi yang dieksekusi disertakan dalam JSON temuan, atau bagian Proses di bawah rincian Runtime. `service.runtimeDetails.process` Untuk jenis temuan ini, biner baru atau yang dimodifikasi adalah`/usr/bin/python3.8`, seperti yang ditunjukkan oleh bidang `service.runtimeDetails.process.executablePath` (Jalur yang dapat dieksekusi).

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

PrivilegeEscalation:Runtime/DockerSocketAccessed

Sebuah proses di dalam kontainer berkomunikasi dengan daemon Docker menggunakan soket Docker.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Soket Docker adalah Soket Domain Unix yang digunakan daemon Docker (`dockerd`) untuk berkomunikasi dengan kliennya. Sebuah klien dapat melakukan berbagai tindakan, seperti membuat kontainer dengan berkomunikasi dengan daemon Docker melalui soket Docker. Proses kontainer yang mengakses soket Docker adalah hal yang mencurigakan. Proses kontainer dapat keluar dari wadah dan mendapatkan akses tingkat host dengan berkomunikasi dengan soket Docker dan membuat wadah istimewa.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

PrivilegeEscalation:Runtime/RuncContainerEscape

Percobaan melarikan diri dari kontainer melalui runC terdeteksi.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

runC adalah runtime kontainer tingkat rendah yang digunakan runtime kontainer tingkat tinggi, seperti Docker dan Containerd untuk menelurkan dan menjalankan container. RunC selalu dijalankan dengan hak akses root karena perlu melakukan tugas tingkat rendah untuk membuat wadah. Aktor ancaman dapat memperoleh akses tingkat host dengan memodifikasi atau mengeksploitasi kerentanan dalam biner runC.

Temuan ini mendeteksi modifikasi biner runC dan upaya potensial untuk mengeksploitasi kerentanan RuNC berikut:

- CVE-2019-5736— Eksploitasi CVE-2019-5736 melibatkan penimpaan biner runC dari dalam wadah. Temuan ini dipanggil ketika biner runC dimodifikasi oleh proses di dalam wadah.
- CVE-2024-21626Eksploitasi CVE-2024-21626 melibatkan pengaturan direktori kerja saat ini (CWD) atau wadah ke deskriptor file terbuka. `/proc/self/fd/`*`FileDescriptor`* Temuan ini dipanggil ketika proses kontainer dengan direktori kerja saat ini di bawah `/proc/self/fd/` terdeteksi, misalnya,`/proc/self/fd/7`.

Temuan ini mungkin menunjukkan bahwa pelaku berbahaya telah berusaha melakukan eksploitasi di salah satu jenis kontainer berikut:

- Sebuah kontainer baru dengan citra yang dikendalikan penyerang.
- Kontainer yang sudah ada yang sebelumnya dapat diakses oleh pelaku dengan izin tulis pada biner runC tingkat host.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Percobaan melarikan diri dari kontainer melalui agen rilis CGroups terdeteksi.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa percobaan untuk memodifikasi file agen rilis grup kontrol (cgroup) telah terdeteksi. Linux menggunakan grup kontrol (cgroup) untuk membatasi, menghitung, dan mengisolasi penggunaan sumber daya dari kumpulan proses. Setiap cgroup memiliki file agen rilis (`release_agent`), yaitu skrip yang dijalankan Linux ketika proses apa pun di dalam cgroup berakhir. File agen rilis selalu dijalankan di tingkat host. Pelaku ancaman di dalam kontainer dapat melarikan diri ke host dengan menulis perintah arbitrer ke file agen rilis milik cgroup. Ketika proses di dalam cgroup tersebut berakhir, perintah yang ditulis oleh pelaku akan dijalankan.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

DefenseEvasion:Runtime/ProcessInjection.Proc

Sebuah injeksi proses menggunakan sistem file proc terdeteksi dalam kontainer atau instans Amazon EC2.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Injeksi proses adalah teknik yang digunakan pelaku ancaman untuk menginjeksi kode ke dalam proses guna menghindari pertahanan dan berpotensi meningkatkan hak akses. Sistem file proc

(procfs) adalah sistem file khusus di Linux yang menyajikan memori virtual proses dalam bentuk file. Jalur file tersebut adalah `/proc/PID/mem`, di mana `PID` adalah ID unik proses tersebut. Pelaku ancaman dapat menulis ke file ini untuk menginjeksi kode ke dalam proses. Temuan ini mengidentifikasi potensi percobaan untuk menulis ke file ini.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

DefenseEvasion:Runtime/ProcessInjection.Ptrace

Sebuah injeksi proses menggunakan panggilan sistem ptrace terdeteksi di dalam kontainer atau instans Amazon EC2.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Injeksi proses adalah teknik yang digunakan pelaku ancaman untuk menginjeksi kode ke dalam proses guna menghindari pertahanan dan berpotensi meningkatkan hak akses. Suatu proses dapat menggunakan panggilan sistem ptrace untuk menginjeksi kode ke dalam proses lain. Temuan ini mengidentifikasi potensi percobaan untuk menginjeksi kode ke dalam proses menggunakan panggilan sistem ptrace.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

Sebuah injeksi proses melalui penulisan langsung ke memori virtual terdeteksi di dalam kontainer atau instans Amazon EC2.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Injeksi proses adalah teknik yang digunakan pelaku ancaman untuk menginjeksi kode ke dalam proses guna menghindari pertahanan dan berpotensi meningkatkan hak akses. Suatu proses dapat menggunakan panggilan sistem seperti `process_vm_writev` untuk langsung menyuntikkan kode ke memori virtual proses lain. Temuan ini mengidentifikasi upaya potensial untuk menyuntikkan kode ke dalam proses menggunakan panggilan sistem untuk menulis ke memori virtual proses.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Execution:Runtime/ReverseShell

Sebuah proses dalam sebuah kontainer atau sebuah instans Amazon EC2 telah membuat reverse shell.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Reverse shell adalah sesi shell yang dibuat pada koneksi yang dimulai dari host target ke host pelaku. Hal ini berbeda dengan shell normal yang dimulai dari host pelaku ke host target. Pelaku ancaman membuat reverse shell untuk menjalankan perintah pada target setelah mendapatkan akses awal ke target. Temuan ini mengidentifikasi koneksi shell terbalik yang berpotensi mencurigakan.

GuardDuty memeriksa aktivitas dan konteks runtime terkait, dan menghasilkan jenis temuan ini hanya jika aktivitas dan konteks terkait ditemukan tidak biasa atau mencurigakan. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Agen GuardDuty keamanan memantau peristiwa dari berbagai sumber. Untuk mengidentifikasi sumber daya yang terkena dampak, lihat Jenis sumber daya di detail temuan di GuardDuty konsol. Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

DefenseEvasion:Runtime/FilelessExecution

Sebuah proses dalam sebuah kontainer atau sebuah instans Amazon EC2 menjalankan kode dari memori.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda saat sebuah proses dijalankan menggunakan file executable dalam memori pada disk. Ini adalah teknik penghindaran pertahanan umum yang tidak menulis executable berbahaya ke disk untuk menghindari deteksi berbasis pemindaian sistem file. Meskipun teknik ini biasa digunakan oleh malware, teknik ini juga memiliki beberapa kasus penggunaan yang sah. Salah satu contohnya adalah compiler just-in-time (JIT) yang menulis kode yang dikompilasi ke memori dan menjalankannya dari memori.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Impact:Runtime/CryptoMinerExecuted

Kontainer atau instans Amazon EC2 menjalankan file biner yang terkait dengan aktivitas penambangan mata uang kripto.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans atau wadah EC2 yang terdaftar di AWS lingkungan Anda mengeksekusi file biner yang terkait dengan aktivitas penambangan cryptocurrency. Pelaku ancaman dapat berusaha mengambil kendali atas sumber daya komputasi guna memanfaatkannya dengan tujuan jahat untuk penambangan mata uang kripto yang tidak sah.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol dan lihatMemperbaiki temuan Pemantauan Runtime.

Execution:Runtime/NewLibraryLoaded

Pustaka yang baru dibuat atau yang baru saja dimodifikasi telah dimuat oleh sebuah proses di dalam kontainer.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa pustaka dibuat atau dimodifikasi di dalam kontainer selama runtime dan dimuat oleh sebuah proses yang berjalan di dalam kontainer tersebut. Praktik terbaiknya adalah menjaga kontainer tetap imutabel pada saat runtime, dan tidak membuat atau memodifikasi file biner, skrip, atau pustaka selama masa pakai kontainer. Pemuatan pustaka yang baru dibuat

atau dimodifikasi dalam kontainer dapat mengindikasikan aktivitas yang mencurigakan. Perilaku ini menunjukkan bahwa pelaku berbahaya kemungkinan telah mendapatkan akses ke kontainer, telah mengunduh, dan menjalankan malware atau perangkat lunak lain sebagai bagian dari penyusupan yang potensial. Meskipun jenis aktivitas ini bisa menjadi indikasi adanya penyusupan, ini juga merupakan pola penggunaan yang umum. Oleh karena itu, GuardDuty gunakan mekanisme untuk mengidentifikasi contoh mencurigakan dari aktivitas ini dan menghasilkan jenis temuan ini hanya untuk contoh yang mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Sebuah proses di dalam kontainer yang melakukan mounting sistem file host pada saat runtime.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Beberapa teknik pelarian kontainer memerlukan mounting sistem file host di dalam kontainer pada saat runtime. Temuan ini memberi tahu Anda bahwa proses di dalam kontainer yang berpotensi mencoba melakukan mounting sistem file host, yang mungkin menunjukkan percobaan untuk meloloskan diri menuju host.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

PrivilegeEscalation:Runtime/UserfaultfdUsage

Sebuah proses yang digunakan **`userfaultfd`** sistem panggilan untuk menangani kesalahan halaman dalam ruang pengguna.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Biasanya, kesalahan halaman ditangani oleh kernel di ruang kernel. Namun, panggilan sistem `userfaultfd` memungkinkan sebuah proses menangani kesalahan halaman pada sistem file di ruang pengguna. Hal ini adalah fitur berguna yang memungkinkan implementasi sistem file ruang pengguna. Di sisi lain, ini juga dapat digunakan oleh proses yang berpotensi berbahaya untuk menginterupsi kernel dari ruang pengguna. Interupsi kernel menggunakan panggilan sistem `userfaultfd` adalah teknik eksploitasi umum untuk memperluas periode race selama eksploitasi kondisi race kernel. Penggunaan `userfaultfd` dapat mengindikasikan aktivitas mencurigakan pada instans Amazon Elastic Compute Cloud (Amazon EC2).

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Execution:Runtime/SuspiciousTool

Kontainer atau instans Amazon EC2 menjalankan skrip atau file biner yang sering digunakan dalam skenario keamanan ofensif seperti keterlibatan uji penetrasi.

Tingkat keparahan default: Variabel

Tingkat keparahan temuan ini bisa tinggi atau rendah, tergantung pada apakah alat mencurigakan yang terdeteksi dianggap penggunaan ganda atau hanya untuk penggunaan ofensif.

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa alat yang mencurigakan telah dieksekusi pada instans atau wadah EC2 di lingkungan Anda. AWS Hal ini termasuk alat yang digunakan dalam keterlibatan uji penetrasi, juga disebut sebagai alat backdoor, pemindai jaringan, dan sniffer jaringan. Semua alat ini dapat digunakan dalam konteks jinak tetapi juga sering digunakan oleh pelaku ancaman dengan niat jahat. Mengamati alat keamanan ofensif dapat menunjukkan bahwa instans atau wadah EC2 terkait telah dikompromikan.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Execution:Runtime/SuspiciousCommand

Perintah mencurigakan telah dijalankan pada instans Amazon EC2 atau kontainer yang menunjukkan adanya penyusupan.

Tingkat keparahan default: Variabel

Bergantung pada dampak dari pola berbahaya yang diamati, tingkat keparahan tipe temuan ini bisa rendah, sedang, atau tinggi.

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa perintah mencurigakan telah dijalankan dan ini menunjukkan bahwa instans Amazon EC2 atau wadah di lingkungan AWS Anda telah disusupi. Hal ini mungkin berarti bahwa file diunduh dari sumber yang mencurigakan kemudian dijalankan, atau proses yang sedang berjalan menampilkan pola yang diketahui berbahaya di baris perintahnya. Hal ini lebih lanjut menunjukkan bahwa malware sedang berjalan di sistem.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

> **Note**
>
> Argumen baris perintah proses mungkin berisi data sensitif. Untuk melindungi data sensitif, temuan pemantauan GuardDuty runtime tidak menyertakan argumen baris perintah lengkap. Sebagai gantinya, `Service.RuntimeDetails.Context.CommandLineExample` berikan contoh representatif dari pola baris perintah yang menghasilkan temuan.

DefenseEvasion:Runtime/SuspiciousCommand

Perintah telah dijalankan pada instans Amazon EC2 atau kontainer yang tercantum, dan mencoba memodifikasi atau menonaktifkan mekanisme pertahanan Linux, seperti firewall atau layanan sistem penting.

Tingkat keparahan default: Variabel

Bergantung pada mekanisme pertahanan mana yang telah dimodifikasi atau dinonaktifkan, tingkat keparahan tipe temuan ini bisa tinggi, sedang, atau rendah.

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa perintah yang berusaha menyembunyikan serangan dari layanan keamanan sistem lokal, telah dijalankan. Hal ini termasuk tindakan seperti menonaktifkan firewall Unix, memodifikasi tabel IP lokal, menghapus entri crontab, menonaktifkan layanan lokal, atau mengambil alih fungsi `LDPreload`. Setiap modifikasi sangat mencurigakan dan merupakan potensi indikator penyusupan. Oleh karena itu, mekanisme ini mendeteksi atau mencegah penyusupan sistem lebih lanjut.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

DefenseEvasion:Runtime/PtraceAntiDebugging

Proses dalam kontainer atau instans Amazon EC2 telah menjalankan tindakan anti-debugging menggunakan panggilan sistem ptrace.

Tingkat keparahan default: Rendah

- Fitur: Pemantauan Runtime

Temuan ini menunjukkan bahwa proses yang berjalan pada instans Amazon EC2 yang terdaftar atau wadah dalam AWS lingkungan Anda telah menggunakan panggilan sistem ptrace dengan opsi tersebut. `PTRACE_TRACEME` Aktivitas ini akan menyebabkan debugger terlampir terlepas dari proses yang sedang berjalan. Jika tidak ada debugger yang terlampir, maka tidak akan ada efek. Namun, aktivitas itu sendiri menimbulkan kecurigaan. Hal ini mungkin menunjukkan bahwa malware sedang berjalan di sistem. Malware sering menggunakan teknik anti-debugging untuk menghindari analisis, dan teknik ini dapat dideteksi saat runtime.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Execution:Runtime/MaliciousFileExecuted

File executable yang teridentifikasi berbahaya telah dijalankan pada instans Amazon EC2 atau kontainer.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa executable berbahaya yang diketahui telah dieksekusi di instans Amazon EC2 atau wadah dalam lingkungan Anda. AWS Hal ini adalah indikator kuat bahwa instans atau kontainer berpotensi telah disusupi dan malware telah dijalankan.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Execution:Runtime/MaliciousFileExecuted.Custom

File executable berbahaya di daftar ancaman kustom telah dijalankan pada instans Amazon EC2 atau kontainer.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa file yang dapat dieksekusi yang disertakan dalam daftar entitas ancaman yang Anda unggah dan aktifkan telah dieksekusi pada instans Amazon EC2 atau wadah dalam lingkungan Anda. AWS Dalam GuardDuty, daftar entitas ancaman dapat mencakup alamat IP berbahaya yang diketahui, domain, dan hash SHA-256 file. GuardDuty menghasilkan

temuan berdasarkan aktivitas yang terkait dengan daftar entitas ancaman yang diunggah. Anda dapat melihat nama daftar entitas ancaman tersebut di detail temuan.

Catatan: Temuan ini hanya dipicu ketika file executable yang hash-nya tercantum dalam daftar entitas ancaman, dijalankan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Execution:Runtime/SuspiciousShellCreated

Layanan jaringan atau proses yang dapat diakses jaringan pada instans Amazon EC2, atau dalam wadah telah memulai proses shell interaktif.

Tingkat keparahan default: Rendah

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa layanan yang dapat diakses jaringan pada instans Amazon EC2 atau dalam wadah di AWS lingkungan Anda telah meluncurkan shell interaktif. Dalam keadaan tertentu, skenario ini dapat mengindikasikan perilaku pasca-eksploitasi. Shell interaktif memungkinkan penyerang menjalankan perintah arbitrer pada instans atau kontainer yang disusupi.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut. Anda dapat melihat informasi proses yang dapat diakses jaringan di detail proses induk.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

PrivilegeEscalation:Runtime/ElevationToRoot

Proses yang berjalan pada instans atau penampung Amazon EC2 yang terdaftar telah mengasumsikan hak akses root.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan di Amazon EC2 yang terdaftar atau dalam wadah yang terdaftar di lingkungan AWS Anda telah mengambil hak akses root melalui eksekusi biner yang tidak biasa atau `setuid` mencurigakan. Ini menunjukkan bahwa proses yang sedang berjalan berpotensi dikompromikan, untuk instans EC2 melalui eksploitasi, atau melalui eksploitasi. `setuid` Dengan menggunakan hak akses root, penyerang berpotensi mengeksekusi perintah pada instance atau container.

Meskipun GuardDuty dirancang untuk tidak menghasilkan jenis temuan ini untuk aktivitas yang melibatkan penggunaan `sudo` perintah secara teratur, itu akan menghasilkan temuan ini ketika mengidentifikasi aktivitas sebagai tidak biasa atau mencurigakan.

GuardDuty memeriksa aktivitas dan konteks runtime terkait, dan menghasilkan jenis temuan ini hanya jika aktivitas dan konteks terkait tidak biasa atau mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Discovery:Runtime/SuspiciousCommand

Perintah mencurigakan telah dijalankan pada instans Amazon EC2 atau dalam wadah, yang memungkinkan penyerang untuk mendapatkan informasi tentang sistem lokal, di sekitarnya AWS infrastruktur, atau infrastruktur kontainer.

Tingkat keparahan default: Rendah

Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans atau wadah Amazon EC2 yang terdaftar di lingkungan AWS Anda telah menjalankan perintah yang mungkin memberi penyerang informasi penting untuk berpotensi memajukan serangan. Informasi berikut mungkin telah diambil:

- Sistem lokal seperti konfigurasi pengguna atau jaringan,
- AWS Sumber daya dan izin lain yang tersedia, atau
- Infrastruktur Kubernetes seperti layanan dan pod.

Instans Amazon EC2 atau wadah yang tercantum dalam detail temuan mungkin telah disusupi.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Anda dapat menemukan detail tentang perintah mencurigakan di bidang `service.runtimeDetails.context` JSON temuan. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Persistence:Runtime/SuspiciousCommand

Perintah mencurigakan telah dijalankan pada instans Amazon EC2 atau dalam wadah, yang memungkinkan penyerang untuk mempertahankan akses dan kontrol di AWS lingkungan.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans Amazon EC2 yang terdaftar atau dalam wadah di lingkungan AWS Anda telah menjalankan perintah yang mencurigakan. Perintah ini menginstal metode persistensi yang memungkinkan malware berjalan tanpa gangguan, atau memungkinkan penyerang untuk terus mengakses instance atau tipe sumber daya kontainer yang berpotensi dikompromikan. Ini berpotensi berarti bahwa layanan sistem telah

diinstal atau dimodifikasi, `crontab` telah dimodifikasi, atau pengguna baru telah ditambahkan ke konfigurasi sistem.

GuardDuty memeriksa aktivitas dan konteks runtime terkait, dan menghasilkan jenis temuan ini hanya jika aktivitas dan konteks terkait tidak biasa atau mencurigakan.

Instans Amazon EC2 atau wadah yang tercantum dalam detail temuan mungkin telah disusupi.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Anda dapat menemukan detail tentang perintah mencurigakan di bidang `service.runtimeDetails.context` JSON temuan. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

PrivilegeEscalation:Runtime/SuspiciousCommand

Perintah mencurigakan telah dijalankan pada instans Amazon EC2 atau dalam wadah, yang memungkinkan penyerang untuk meningkatkan hak istimewa.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada instans Amazon EC2 yang terdaftar atau dalam wadah di lingkungan AWS Anda telah menjalankan perintah yang mencurigakan. Perintah mencoba untuk melakukan eskalasi hak istimewa, yang memungkinkan musuh untuk melakukan tugas-tugas hak istimewa yang tinggi.

GuardDuty memeriksa aktivitas dan konteks runtime terkait, dan menghasilkan jenis temuan ini hanya jika aktivitas dan konteks terkait tidak biasa atau mencurigakan.

Instans Amazon EC2 atau wadah yang tercantum dalam detail temuan mungkin telah disusupi.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol.

Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

DefenseEvasion:Runtime/KernelModuleLoaded

Modul kernel dimuat pada instans Amazon EC2, yang menunjukkan upaya untuk mendapatkan akses tingkat kernel.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini menunjukkan bahwa sebuah modul kernel dimuat pada instans EC2 tercantum. Karena modul kernel memiliki hak akses tingkat sistem tertinggi (ring 0), ini dapat menunjukkan bahwa pelaku ancaman telah memperoleh akses tingkat kernel. Tingkat akses ini memungkinkan kontrol penuh atas sistem.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Persistence:Runtime/SensitiveFileModified

File sistem yang sensitif dari segi keamanan telah dimodifikasi pada kontainer atau instans Amazon EC2, yang berpotensi memungkinkan musuh untuk mendapatkan persistensi.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa file sistem yang sensitif dari segi keamanan pada kontainer atau instans Amazon EC2 telah dimodifikasi, yang berpotensi memungkinkan musuh mempertahankan hak pelaksanaan persisten pada sistem. Ini dapat mencakup instalasi file kunci SSH baru, perubahan pada file konfigurasi pengguna, modifikasi file bayangan atau kata sandi, pembuatan tugas terjadwal, manipulasi skrip startup sistem, atau modifikasi file yang dapat dieksekusi atau skrip oleh proses layanan web dalam konteks yang mencurigakan. Modifikasi ini adalah indikator kompromi yang dapat memungkinkan persistensi yang tidak sah di lingkungan Anda.

GuardDuty memantau file sistem sensitif keamanan yang sering ditargetkan oleh musuh untuk ketekunan. Karena file-file ini juga dapat dimodifikasi selama administrasi dan manajemen sistem yang sah, GuardDuty memeriksa aktivitas dan konteks runtime terkait untuk menghasilkan temuan ini hanya ketika modifikasi berkorelasi dengan aktivitas mencurigakan lainnya.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Bidang `service.runtimeDetails.context` berisi rincian tentang modifikasi file yang mencurigakan, termasuk jalur file dan jenis operasi.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

PrivilegeEscalation:Runtime/SensitiveFileModified

File sistem yang sensitif dari segi keamanan telah dimodifikasi pada kontainer atau instans Amazon EC2, yang berpotensi memungkinkan musuh untuk meningkatkan hak istimewa.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa file sistem yang sensitif dari segi keamanan telah dimodifikasi pada kontainer atau instans Amazon EC2, yang berpotensi memungkinkan musuh untuk meningkatkan hak istimewa mereka di sistem. Ini dapat melibatkan modifikasi pada file yang penting dari segi keamanan seperti konfigurasi sudoers, pengaturan PAM, atau file autentikasi sistem. Modifikasi ini adalah indikator kompromi yang dapat memungkinkan eskalasi hak istimewa yang tidak sah, yang berpotensi mengakibatkan akses root yang tidak sah, mekanisme autentikasi yang melemah, atau kontrol keamanan yang berkurang.

GuardDuty memantau file sistem sensitif keamanan yang sering ditargetkan oleh musuh untuk eskalasi hak istimewa. Karena file-file ini juga dapat dimodifikasi selama administrasi dan manajemen sistem yang sah, GuardDuty memeriksa aktivitas dan konteks runtime terkait untuk menghasilkan temuan ini hanya ketika modifikasi berkorelasi dengan aktivitas mencurigakan lainnya.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Bidang `service.runtimeDetails.context` berisi rincian tentang modifikasi file yang mencurigakan, termasuk jalur file dan jenis operasi.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

DefenseEvasion:Runtime/SensitiveFileModified

File sistem yang sensitif dari segi keamanan telah dimodifikasi pada kontainer atau instans Amazon EC2, yang berpotensi memungkinkan musuh untuk menghindari deteksi.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa file sistem yang sensitif dari segi keamanan pada kontainer atau instans Amazon EC2 telah dimodifikasi, yang berpotensi memungkinkan musuh untuk menghindari deteksi di sistem. Ini bisa melibatkan modifikasi pada file log sistem, konfigurasi audit, file riwayat perintah, atau log sistem. Modifikasi ini adalah indikator kompromi yang dapat memungkinkan penyembunyian aktivitas yang tidak sah, gangguan pemantauan keamanan, atau penghapusan bukti aktivitas sistem.

GuardDuty memantau file sistem sensitif keamanan yang sering ditargetkan oleh musuh untuk penghindaran pertahanan. Karena file-file ini juga dapat dimodifikasi selama administrasi dan manajemen sistem yang sah, GuardDuty memeriksa aktivitas dan konteks runtime terkait untuk menghasilkan temuan ini hanya ketika modifikasi berkorelasi dengan aktivitas mencurigakan lainnya.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Bidang `service.runtimeDetails.context` berisi rincian tentang modifikasi file yang mencurigakan, termasuk jalur file dan jenis operasi.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Menemukan jenis yang memerlukan Aturan Deteksi Kustom

GuardDuty menghasilkan jenis temuan berikut hanya jika Anda mengaktifkan Aturan Deteksi Kustom untuk Pemantauan Waktu Proses. Untuk informasi selengkapnya, lihat Aturan Deteksi Kustom di GuardDuty.

Setiap temuan mencakup `CustomDetectionRuleName` bidang, yang berisi nama aturan yang menghasilkan temuan.

Topik

- CommandAndControl:Runtime/SuspiciousCommand
- CredentialAccess:Runtime/SensitiveFileRead
- Discovery:Runtime/SensitiveFileRead
- Exfiltration:Runtime/SuspiciousCommand

CommandAndControl:Runtime/SuspiciousCommand

Proses pada instans Amazon EC2 atau dalam wadah menjalankan perintah mencurigakan yang dapat digunakan penyerang untuk berkomunikasi dengan dan mengontrol sumber daya.

Tingkat keparahan default: Variabel

Tingkat keparahan tergantung pada aturan yang menghasilkan temuan: tinggi untuk DnsTunnelingToolExecuted dan sedang untukSuspiciousProtocolTunneling.

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses pada instans atau wadah Amazon EC2 di lingkungan AWS Anda menjalankan perintah yang dapat digunakan penyerang untuk berkomunikasi dengan sumber daya yang disusupi sambil menghindari deteksi. Misalnya, proses mungkin telah menjalankan alat yang mengalirkan lalu lintas melalui DNS, atau yang mengekspos sumber daya melalui terowongan atau layanan proxy.

GuardDuty menghasilkan temuan ini dari DnsTunnelingToolExecuted dan SuspiciousProtocolTunneling aturan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

CredentialAccess:Runtime/SensitiveFileRead

Proses pada instans Amazon EC2 atau dalam wadah mengakses file sensitif yang mungkin berisi kredensyal.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses pada instans atau penampung Amazon EC2 di lingkungan AWS Anda mengakses file sensitif keamanan yang mungkin berisi kredensyal atau rahasia lainnya. Misalnya, proses mungkin telah mengakses memori proses lain melalui sistem `/proc` file untuk mengekstrak kredensialnya.

GuardDuty menghasilkan temuan ini dari DumpProcessMemoryFromProc aturan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Discovery:Runtime/SensitiveFileRead

Proses pada instans Amazon EC2 atau dalam wadah mengakses file sensitif yang berisi informasi tentang pengguna lokal dan kredensyal.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses pada instans atau wadah Amazon EC2 di lingkungan AWS Anda mengakses file sistem yang sensitif terhadap keamanan, seperti akun pengguna lokal

atau file hash kata sandi. Penyerang dapat menggunakan informasi ini untuk menemukan akun dan mencoba memecahkan kata sandi mereka.

GuardDuty menghasilkan temuan ini dari PasswordShadowFileDiscovery aturan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Pemantauan Runtime.

Exfiltration:Runtime/SuspiciousCommand

Proses pada instans Amazon EC2 atau dalam wadah menjalankan perintah mencurigakan yang dapat digunakan penyerang untuk memindahkan data dari lingkungan Anda.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses pada instans atau penampung Amazon EC2 di lingkungan AWS Anda menjalankan perintah yang berpotensi digunakan untuk memindahkan data dari lingkungan Anda. Misalnya, proses mungkin telah mengunggah file ke endpoint eksternal atau layanan penyimpanan cloud, atau membagi data menjadi potongan-potongan kecil untuk menghindari batas transfer.

GuardDuty menghasilkan temuan ini dariCurlWgetExfiltrateData,DataSplittingForExfiltration, dan S3DataExfiltrationWithRclone aturan.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Lihat informasi yang lebih lengkap di Memperbaiki temuan Pemantauan Runtime.

Perlindungan Malware untuk jenis pencarian EC2

GuardDuty Perlindungan Malware untuk EC2 menyediakan Perlindungan Malware tunggal untuk penemuan EC2 untuk semua ancaman yang terdeteksi selama pemindaian instans EC2 atau beban kerja kontainer. Temuan ini mencakup jumlah total deteksi yang dilakukan selama pemindaian, dan berdasarkan tingkat keparahannya, memberikan rincian untuk 32 ancaman teratas yang dideteksi. Tidak seperti GuardDuty temuan lain, Perlindungan Malware untuk temuan EC2 tidak diperbarui ketika instans EC2 atau beban kerja kontainer yang sama dipindai lagi.

Perlindungan Malware baru untuk temuan EC2 dihasilkan untuk setiap pemindaian yang mendeteksi malware. Perlindungan Malware untuk temuan EC2 mencakup informasi tentang pemindaian yang sesuai yang menghasilkan temuan serta GuardDuty temuan yang memulai pemindaian ini. Ini membuatnya lebih mudah untuk menghubungkan perilaku mencurigakan dengan malware yang terdeteksi.

> **Note**
>
> Saat GuardDuty mendeteksi aktivitas berbahaya pada beban kerja kontainer, Perlindungan Malware untuk EC2 tidak menghasilkan temuan tingkat EC2.

Temuan berikut khusus untuk Perlindungan GuardDuty Malware untuk EC2.

Topik

- Execution:EC2/MaliciousFile
- Execution:ECS/MaliciousFile
- Execution:Kubernetes/MaliciousFile
- Execution:Container/MaliciousFile
- Execution:EC2/SuspiciousFile
- Execution:ECS/SuspiciousFile
- Execution:Kubernetes/SuspiciousFile
- Execution:Container/SuspiciousFile

Execution:EC2/MaliciousFile

File berbahaya telah terdeteksi pada instans EC2.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file berbahaya pada instans EC2 yang terdaftar di lingkungan Anda AWS . Instans yang tercantum ini mungkin disusupi. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Execution:ECS/MaliciousFile

File berbahaya telah terdeteksi pada cluster ECS.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file berbahaya pada beban kerja kontainer milik cluster ECS. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kontainer milik klaster ECS mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki cluster ECS yang berpotensi dikompromikan.

Execution:Kubernetes/MaliciousFile

File berbahaya telah terdeteksi pada klaster Kubernetes.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file berbahaya pada beban kerja kontainer milik cluster Kubernetes. Jika ini adalah cluster yang dikelola EKS, detail temuan akan memberikan informasi tambahan tentang sumber daya EKS yang terkena dampak. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Execution:Container/MaliciousFile

File berbahaya telah terdeteksi pada kontainer mandiri.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file berbahaya pada beban kerja kontainer dan tidak ada informasi cluster yang diidentifikasi. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki wadah mandiri yang berpotensi dikompromikan.

Execution:EC2/SuspiciousFile

File mencurigakan telah terdeteksi pada instans EC2.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file mencurigakan pada instans EC2. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Deteksi jenis `SuspiciousFile` menunjukkan bahwa program yang berpotensi tidak diinginkan, seperti adware, spyware, atau alat penggunaan ganda, muncul pada sumber daya yang terpengaruh. Program-program ini dapat berdampak negatif pada sumber daya Anda, atau digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh penyerang sebagai alat peretas untuk mencoba menyusupi sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Execution:ECS/SuspiciousFile

File mencurigakan telah terdeteksi pada cluster ECS.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file mencurigakan pada wadah milik cluster ECS. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Deteksi jenis `SuspiciousFile` menunjukkan bahwa program yang berpotensi tidak diinginkan, seperti adware, spyware, atau alat penggunaan ganda, muncul pada sumber daya yang terpengaruh. Program-program ini dapat berdampak negatif pada sumber daya Anda, atau digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh penyerang sebagai alat peretas untuk mencoba menyusupi sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kontainer milik klaster ECS mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki cluster ECS yang berpotensi dikompromikan.

Execution:Kubernetes/SuspiciousFile

File mencurigakan telah terdeteksi pada klaster Kubernetes.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file mencurigakan pada wadah milik cluster Kubernetes. Jika ini adalah

cluster yang dikelola EKS, detail temuan akan memberikan informasi tambahan tentang EKS yang terkena dampak. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Deteksi jenis `SuspiciousFile` menunjukkan bahwa program yang berpotensi tidak diinginkan, seperti adware, spyware, atau alat penggunaan ganda, muncul pada sumber daya yang terpengaruh. Program-program ini dapat berdampak negatif pada sumber daya Anda, atau digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh penyerang sebagai alat peretas untuk mencoba menyusupi sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Execution:Container/SuspiciousFile

File mencurigakan telah terdeteksi pada kontainer mandiri.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file mencurigakan pada wadah tanpa informasi cluster. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Deteksi jenis `SuspiciousFile` menunjukkan bahwa program yang berpotensi tidak diinginkan, seperti adware, spyware, atau alat penggunaan ganda, muncul pada sumber daya yang terpengaruh. Program-program ini dapat berdampak negatif pada sumber daya Anda, atau digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh penyerang sebagai alat peretas untuk mencoba menyusupi sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin disusupi. Lihat informasi yang lebih lengkap di Memperbaiki wadah mandiri yang berpotensi dikompromikan.

Perlindungan Malware untuk tipe pencarian S3

GuardDuty menghasilkan temuan hanya ketika mendeteksi potensi ancaman keamanan di Anda Akun AWS. Perlindungan Malware untuk temuan S3 menunjukkan bahwa objek yang diunggah yang memulai pemindaian malware berisi file yang berpotensi berbahaya.

GuardDuty Agar Amazon dapat menghasilkan temuan di Anda Akun AWS, aktifkan keduanya GuardDuty dan Perlindungan Malware untuk S3. Praktik terbaik adalah mengaktifkan terlebih dahulu GuardDuty dan kemudian Perlindungan Malware untuk S3. Jika pesanan ini berbeda untuk Anda, pastikan untuk mengaktifkan GuardDuty sebelum objek S3 diunggah ke bucket Anda yang dilindungi.

> **Note**
>
> GuardDuty tidak dapat menghasilkan temuan untuk objek S3 yang dipindai sebelum Anda mengaktifkan. GuardDuty Untuk memindai objek S3 yang ada, Anda dapat mengunggahnya lagi.

Object:S3/MaliciousFile

File berbahaya telah terdeteksi pada objek S3 yang dipindai.

Tingkat keparahan default: Tinggi

- Fitur: Perlindungan Malware untuk S3

Temuan ini menunjukkan bahwa pemindaian malware telah mendeteksi objek S3 yang tercantum adalah berbahaya. Untuk informasi selengkapnya, lihat bagian Ancaman terdeteksi di panel rincian pencarian.

Remediasi rekomendasi:

Jika temuan ini tidak terduga, objek S3 tersebut berpotensi berbahaya. Untuk informasi tentang langkah-langkah remediasi yang direkomendasikan, lihatMemperbaiki objek S3 yang berpotensi berbahaya.

Perlindungan Malware untuk jenis pencarian Backup

GuardDuty Perlindungan Malware untuk Backup menyediakan satu temuan untuk semua ancaman yang terdeteksi selama pemindaian sumber daya yang diminta. Temuan ini mencakup jumlah total deteksi yang dilakukan selama pemindaian, dan berdasarkan tingkat keparahannya, memberikan rincian untuk 32 ancaman teratas yang dideteksi. Tidak seperti GuardDuty temuan lain, temuan Perlindungan Malware untuk Cadangan tidak diperbarui ketika sumber daya yang sama dipindai lagi. Penemuan Perlindungan Malware untuk Cadangan baru dihasilkan untuk setiap pemindaian yang mendeteksi malware.

Temuan berikut khusus untuk Perlindungan GuardDuty Malware untuk Backup.

Topik

- Execution:EC2/MaliciousFile!Snapshot
- Execution:EC2/MaliciousFile!AMI
- Execution:EC2/MaliciousFile!RecoveryPoint
- Execution:S3/MaliciousFile!RecoveryPoint

Execution:EC2/MaliciousFile!Snapshot

File berbahaya telah terdeteksi dalam snapshot EBS.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware untuk Backup

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk Pemindaian Cadangan telah mendeteksi satu atau lebih file berbahaya dalam snapshot EBS di lingkungan Anda. Untuk informasi lebih lanjut, lihat bagian Ancaman terdeteksi di panel detail temuan.

Rekomendasi remediasi:

Jika ini di luar ekspektasi, snapshot Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki Snapshot EBS yang berpotensi dikompromikan.

Execution:EC2/MaliciousFile!AMI

File berbahaya telah terdeteksi pada AMI EC2.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware untuk Backup

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk Pemindaian Cadangan telah mendeteksi satu atau lebih file berbahaya di AMI di lingkungan Anda. Untuk informasi lebih lanjut, lihat bagian Ancaman terdeteksi di panel detail temuan.

Rekomendasi remediasi:

Jika ini di luar ekspektasi, AMI Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki AMI EC2 yang berpotensi dikompromikan.

Execution:EC2/MaliciousFile!RecoveryPoint

File berbahaya telah terdeteksi di AWS Backup EC2 Recovery Point.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware untuk Backup

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk Pemindaian Cadangan telah mendeteksi satu atau lebih file berbahaya di titik pemulihan EC2 di lingkungan Anda. Titik Pemulihan yang terkena dampaknya bisa jadi adalah snapshot EBS atau AMI EC2. Untuk informasi lebih lanjut, lihat bagian Ancaman terdeteksi di panel detail temuan.

Rekomendasi remediasi:

Jika ini di luar ekspektasi, titik pemulihan EC2 Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat Memperbaiki Titik Pemulihan EC2 yang berpotensi terganggu.

Execution:S3/MaliciousFile!RecoveryPoint

File berbahaya telah terdeteksi di AWS Backup S3 Recovery Point.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware untuk Backup

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk Pemindaian Cadangan telah mendeteksi satu atau lebih objek berbahaya di Titik Pemulihan S3 di lingkungan Anda. Untuk informasi lebih lanjut, lihat bagian Ancaman terdeteksi di panel detail temuan.

Rekomendasi remediasi:

Jika ini di luar ekspektasi, titik pemulihan S3 Anda mungkin telah disusupi. Lihat informasi yang lebih lengkap di Memperbaiki Titik Pemulihan S3 yang berpotensi dikompromikan.

GuardDuty Jenis temuan Perlindungan RDS

GuardDuty RDS Protection mendeteksi perilaku login anomali pada instance database Anda. Temuan berikut khusus untuk Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung dan akan memiliki Jenis Sumber Daya `RDSDBInstance` atau`RDSLimitlessDB`. Tingkat keparahan dan detail temuan akan berbeda berdasarkan jenis temuan.

Topik

- CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin
- CredentialAccess:RDS/AnomalousBehavior.FailedLogin
- CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce
- CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin
- CredentialAccess:RDS/MaliciousIPCaller.FailedLogin
- Discovery:RDS/MaliciousIPCaller
- CredentialAccess:RDS/TorIPCaller.SuccessfulLogin
- CredentialAccess:RDS/TorIPCaller.FailedLogin
- Discovery:RDS/TorIPCaller
- Exfiltration:RDS/AnomalousBehavior
- Impact:RDS/AnomalousBehavior.Drop
- Impact:RDS/AnomalousBehavior.Delete
- Exfiltration:RDS/MaliciousIPCaller
- Exfiltration:RDS/TorIPCaller

- Impact:RDS/MaliciousIPCaller
- Impact:RDS/TorIPCaller

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Seorang pengguna berhasil masuk ke database RDS di akun Anda dengan cara yang anomali.

Tingkat keparahan default: Variabel

> **Note**
>
> Bergantung pada perilaku beranomali yang terkait dengan temuan ini, tingkat keparahan default-nya dapat Rendah, Sedang, dan Tinggi.
>
> - Rendah – Jika nama pengguna yang terkait dengan temuan ini masuk dari alamat IP yang dikaitkan dengan jaringan privat.
> - Sedang – Jika nama pengguna yang terkait dengan temuan ini masuk dari alamat IP publik.
> - Tinggi – Jika ada pola konsisten dalam percobaan masuk yang gagal dari alamat IP publik yang mengindikasikan kebijakan akses yang terlalu permisif.

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa login yang berhasil anomali diamati pada database RDS di lingkungan Anda. AWS Hal ini mungkin menunjukkan bahwa pengguna yang tidak diketahui masuk ke basis data RDS untuk pertama kalinya. Skenario umum adalah pengguna internal yang masuk ke database yang diakses secara terprogram oleh aplikasi dan bukan oleh pengguna individu.

Login yang berhasil ini diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua peristiwa login database di Anda Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML tersebut melacak berbagai faktor aktivitas login RDS, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan detail koneksi basis data tertentu yang digunakan. Untuk informasi tentang peristiwa login yang berpotensi tidak biasa, lihatAnomali berbasis aktivitas login RDS.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, sebaiknya ubah kata sandi pengguna basis data terkait, dan tinjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang beranomali. Temuan tingkat keparahan sedang dan tinggi dapat mengindikasikan bahwa ada kebijakan akses yang terlalu permisif ke basis data, dan kredensial pengguna mungkin telah terekspos atau disusupi. Sebaiknya tempatkan basis data di VPC privat dan batasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil.

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Satu atau lebih upaya login gagal yang tidak biasa diamati pada database RDS di akun Anda.

Tingkat keparahan default: Rendah

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa satu atau lebih login gagal anomali diamati pada database RDS di lingkungan Anda. AWS Percobaan login yang gagal dari alamat IP publik dapat menunjukkan bahwa basis data RDS di akun Anda telah mengalami percobaan serangan brute force oleh pelaku yang berpotensi berbahaya.

Login yang gagal ini diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua peristiwa login database di Anda Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML tersebut melacak berbagai faktor aktivitas login RDS, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan detail koneksi basis data tertentu yang digunakan. Untuk informasi tentang aktivitas login RDS yang berpotensi tidak biasa, lihatAnomali berbasis aktivitas login RDS.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, hal tersebut mungkin menandakan bahwa basis data terekspos secara publik atau terdapat kebijakan akses ke basis data yang terlalu permisif. Sebaiknya tempatkan basis data di VPC privat dan batasi aturan grup keamanan untuk mengizinkan

lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal.

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Seorang pengguna berhasil login ke basis data RDS di akun Anda dari alamat IP publik dengan cara yang beranomali setelah munculnya pola konsisten dalam percobaan login gagal yang tidak biasa.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa indikasi login anomali dari kekuatan kasar yang berhasil diamati pada database RDS di lingkungan Anda. AWS Sebelum adanya login berhasil yang beranomali, pola konsisten dalam percobaan login gagal yang tidak biasa telah diamati. Hal ini menunjukkan bahwa pengguna dan kata sandi yang terkait dengan basis data RDS di akun Anda mungkin telah disusupi, dan basis data RDS tersebut mungkin telah diakses oleh pelaku yang berpotensi berbahaya.

Login brute force yang berhasil ini diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua peristiwa login database di Anda Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML tersebut melacak berbagai faktor aktivitas login RDS, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan detail koneksi basis data tertentu yang digunakan. Untuk informasi tentang aktivitas login RDS yang berpotensi tidak biasa, lihatAnomali berbasis aktivitas login RDS.

Rekomendasi perbaikan:

Aktivitas ini menunjukkan bahwa kredensial basis data mungkin telah terekspos atau disusupi. Sebaiknya ubah kata sandi pengguna basis data terkait, dan tinjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang berpotensi disusupi. Pola konsisten dalam percobaan login gagal yang tidak biasa menunjukkan kebijakan akses yang terlalu permisif ke basis data atau basis data ini mungkin juga telah terekspos secara publik. Sebaiknya tempatkan basis data di VPC privat dan batasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil.

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Seorang pengguna berhasil login ke basis data RDS di akun Anda dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa aktivitas login RDS yang berhasil terjadi dari alamat IP yang dikaitkan dengan aktivitas berbahaya yang diketahui di lingkungan Anda AWS . Hal ini menunjukkan bahwa pengguna dan kata sandi yang terkait dengan basis data RDS di akun Anda mungkin telah disusupi, dan basis data RDS tersebut mungkin telah diakses oleh pelaku yang berpotensi berbahaya.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, hal tersebut mungkin menandakan bahwa kredensial pengguna telah terekspos atau disusupi. Sebaiknya ubah kata sandi pengguna basis data terkait, dan tinjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang disusupi. Aktivitas ini juga dapat menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke basis data atau basis data tersebut terekspos secara publik. Sebaiknya tempatkan basis data di VPC privat dan batasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil.

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Alamat IP yang dikaitkan dengan aktivitas berbahaya yang diketahui gagal mencoba login ke basis data RDS di akun Anda.

Tingkat keparahan default: Medium

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP yang terkait dengan aktivitas berbahaya yang diketahui mencoba masuk ke database RDS di AWS lingkungan Anda, tetapi gagal memberikan

nama pengguna atau kata sandi yang benar. Hal ini menunjukkan bahwa pelaku yang berpotensi berbahaya mungkin mencoba menyusupi basis data RDS di akun Anda.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, hal tersebut mungkin menandakan bahwa terdapat kebijakan akses ke basis data yang terlalu permisif atau basis data terekspos secara publik. Sebaiknya tempatkan basis data di VPC privat dan batasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal.

Discovery:RDS/MaliciousIPCaller

Alamat IP yang dikaitkan dengan aktivitas berbahaya yang diketahui memeriksa basis data RDS di akun Anda; tidak ada percobaan autentikasi yang dilakukan.

Tingkat keparahan default: Medium

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP yang terkait dengan aktivitas berbahaya yang diketahui menyelidiki database RDS di AWS lingkungan Anda, meskipun tidak ada upaya login yang dilakukan. Hal ini mungkin menunjukkan bahwa pelaku yang berpotensi berbahaya mencoba memindai infrastruktur yang dapat diakses publik.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, hal tersebut mungkin menandakan bahwa terdapat kebijakan akses ke basis data yang terlalu permisif atau basis data terekspos secara publik. Sebaiknya tempatkan basis data di VPC privat dan batasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal.

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Seorang pengguna berhasil login ke basis data RDS di akun Anda dari alamat IP simpul keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa pengguna berhasil masuk ke basis data RDS di lingkungan AWS Anda dari alamat IP simpul keluar Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke sumber daya RDS di akun Anda, dengan maksud menyembunyikan identitas asli pengguna anonim.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, hal tersebut mungkin menandakan bahwa kredensial pengguna telah terekspos atau disusupi. Sebaiknya ubah kata sandi pengguna basis data terkait, dan tinjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang disusupi. Aktivitas ini juga dapat menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke basis data atau basis data tersebut terekspos secara publik. Sebaiknya tempatkan basis data di VPC privat dan batasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil.

CredentialAccess:RDS/TorIPCaller.FailedLogin

Sebuah alamat IP Tor mencoba, tetapi gagal login ke basis data RDS di akun Anda.

Tingkat keparahan default: Medium

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP node keluar Tor mencoba masuk ke database RDS di AWS lingkungan Anda, tetapi gagal memberikan nama pengguna atau kata sandi yang benar. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke sumber daya RDS di akun Anda, dengan maksud menyembunyikan identitas asli pengguna anonim.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, hal tersebut mungkin menandakan bahwa terdapat kebijakan akses ke basis data yang terlalu permisif atau basis data terekspos secara publik.

Sebaiknya tempatkan basis data di VPC privat dan batasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal.

Discovery:RDS/TorIPCaller

Alamat IP simpul keluar Tor memeriksa basis data RDS di akun Anda, tidak ada percobaan autentikasi yang dilakukan.

Tingkat keparahan default: Medium

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP simpul keluar Tor memeriksa basis data RDS di lingkungan AWS Anda, meskipun tidak ada percobaan login yang dilakukan. Hal ini mungkin menunjukkan bahwa pelaku yang berpotensi berbahaya mencoba memindai infrastruktur yang dapat diakses publik. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan memantulkan komunikasi melalui relay antara serangkaian node jaringan. Simpul Tor terakhir disebut sebagai simpul keluar. Hal ini dapat menunjukkan akses tidak sah ke sumber daya RDS di akun Anda, dengan maksud menyembunyikan identitas asli pelaku yang berpotensi berbahaya.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, hal tersebut mungkin menandakan bahwa terdapat kebijakan akses ke basis data yang terlalu permisif atau basis data terekspos secara publik. Sebaiknya tempatkan basis data di VPC privat dan batasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal.

Exfiltration:RDS/AnomalousBehavior

Aktivitas anomali dari pengguna yang mengekstraksi data dalam jumlah besar dari database RDS di akun Anda.

Tingkat keparahan default: Rendah

> **Note**
>
> Bergantung pada perilaku anomali yang terkait dengan temuan ini, tingkat keparahan default bisa Rendah, Sedang, atau Tinggi.
>
> - Rendah — Jika nama pengguna yang terkait dengan temuan ini dieksekusi `SELECT` pernyataan dari alamat IP yang terkait dengan jaringan pribadi.
> - Medium — Jika nama pengguna yang terkait dengan temuan ini dieksekusi `SELECT` pernyataan dari alamat IP publik.
> - Tinggi - Jika nama pengguna yang terkait dengan temuan ini, `SELECT` pernyataan yang dieksekusi mengembalikan volume baris yang luar biasa besar, dan aktivitas tersebut berasal dari jaringan publik yang sebelumnya tidak terlihat atau dilakukan oleh peran database dengan hak istimewa tinggi atau klien administratif.

- Fitur: Pemantauan Aktivitas RDS DB

Temuan ini memberi tahu Anda bahwa aktivitas database anomali yang konsisten dengan eksfiltrasi data diamati pada database RDS di lingkungan Anda. AWS Ini mungkin menunjukkan bahwa pengguna database memilih jumlah baris yang jauh lebih tinggi dari biasanya, atau bahwa aktivitas tersebut melibatkan atribut database yang sebelumnya tidak terlihat seperti pengguna baru, alamat IP, atau nama database yang berkontribusi pada lonjakan volume. Skenario umum adalah kredensi database yang dikompromikan yang digunakan untuk mengekstrak data melalui kombinasi pola akses yang tidak biasa dan volume kueri yang meningkat.

Kegiatan ini diidentifikasi sebagai anomali dengan model GuardDuty anomaly detection machine learning (ML). Model ML mengevaluasi semua peristiwa aktivitas database di Anda Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor aktivitas database RDS seperti pengguna yang membuat permintaan, kueri yang dieksekusi, volume data yang diakses, dan detail koneksi database spesifik yang digunakan. Untuk informasi tentang aktivitas database yang berpotensi tidak biasa, lihatAnomali berbasis aktivitas data RDS.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk database terkait, disarankan untuk mengubah kata sandi pengguna database terkait, dan meninjau log audit yang tersedia untuk menentukan data apa yang diakses pengguna anomali. Disarankan untuk menempatkan database dalam VPC pribadi dan

membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan aktivitas eksfiltrasi anomali.

Impact:RDS/AnomalousBehavior.Drop

Aktivitas anomali dari pengguna yang menjatuhkan data dari database RDS di akun Anda.

Tingkat keparahan default: Medium

> **Note**
>
> Bergantung pada perilaku anomali yang terkait dengan temuan ini, tingkat keparahan default bisa Sedang atau Tinggi.
>
> - Medium — Jika nama pengguna yang terkait dengan temuan ini mengeksekusi pernyataan anomali`DROP`.
> - Tinggi - Jika nama pengguna yang terkait dengan temuan ini mengeksekusi beberapa `DROP` pernyataan, dan aktivitas berasal dari jaringan publik yang sebelumnya tidak terlihat atau dilakukan oleh peran database hak tinggi atau klien administratif.

- Fitur: Pemantauan Aktivitas RDS DB

Temuan ini memberi tahu Anda bahwa aktivitas database anomali yang konsisten dengan operasi destruktif diamati pada database RDS di lingkungan Anda. AWS Ini mungkin menunjukkan bahwa pengguna database menjatuhkan jumlah tabel atau objek database yang jauh lebih tinggi daripada biasanya, atau bahwa aktivitas tersebut melibatkan atribut database yang sebelumnya tidak terlihat seperti pengguna baru, alamat IP, atau nama aplikasi yang berkontribusi pada operasi destruktif. Skenario umum adalah kredensi database yang dikompromikan yang digunakan untuk menghancurkan struktur database melalui kombinasi pola akses yang tidak biasa dan volume `DROP` pernyataan yang meningkat.

Kegiatan ini diidentifikasi sebagai anomali dengan model GuardDuty anomaly detection machine learning (ML). Model ML mengevaluasi semua peristiwa aktivitas database di Anda Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor

aktivitas database RDS seperti pengguna yang membuat permintaan, pernyataan yang dieksekusi, objek database yang ditargetkan, dan rincian koneksi database spesifik yang digunakan. Untuk informasi tentang aktivitas database yang berpotensi tidak biasa, lihatAnomali berbasis aktivitas data RDS.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk database terkait, disarankan untuk segera mengubah kata sandi pengguna database terkait dan mencabut aksesnya. Tinjau log audit yang tersedia untuk menentukan ruang lingkup objek yang dijatuhkan, dan memulai pemulihan dari cadangan jika perlu. Juga disarankan untuk menempatkan database di VPC pribadi dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan aktivitas destruktif anomali.

Impact:RDS/AnomalousBehavior.Delete

Aktivitas anomali dari pengguna yang menghapus data dari database RDS di akun Anda.

Tingkat keparahan default: Rendah

> **Note**
>
> Bergantung pada perilaku anomali yang terkait dengan temuan ini, tingkat keparahan default bisa Rendah, Sedang, atau Tinggi.
>
> - Rendah — Jika nama pengguna yang terkait dengan temuan ini dieksekusi `DELETE` pernyataan dari alamat IP yang terkait dengan jaringan pribadi.
> - Medium — Jika nama pengguna yang terkait dengan temuan ini dieksekusi `DELETE` pernyataan dari alamat IP publik.
> - Tinggi - Jika nama pengguna yang terkait dengan temuan ini, `DELETE` pernyataan yang dieksekusi mengembalikan volume baris yang luar biasa besar, dan aktivitas tersebut berasal dari jaringan publik yang sebelumnya tidak terlihat atau dilakukan oleh peran database dengan hak istimewa tinggi atau klien administratif.

- Fitur: Pemantauan Aktivitas RDS DB

Temuan ini memberi tahu Anda bahwa aktivitas database anomali yang konsisten dengan operasi destruktif diamati pada database RDS di lingkungan Anda. AWS Ini mungkin menunjukkan bahwa pengguna database menghapus jumlah baris yang jauh lebih tinggi dari biasanya, atau bahwa aktivitas tersebut melibatkan atribut database yang sebelumnya tidak terlihat, seperti pengguna baru, alamat IP, atau nama aplikasi, yang berkontribusi pada operasi destruktif. Skenario umum adalah kredensi database yang dikompromikan yang digunakan untuk menghapus data secara sistematis melalui kombinasi pola akses yang tidak biasa dan volume pernyataan yang meningkat`DELETE`.

Kegiatan ini diidentifikasi sebagai anomali dengan model GuardDuty anomaly detection machine learning (ML). Model ML mengevaluasi semua peristiwa aktivitas database di Anda Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor aktivitas database RDS seperti pengguna yang membuat permintaan, pernyataan yang dieksekusi, jumlah baris yang terpengaruh, dan detail koneksi database spesifik yang digunakan. Untuk informasi tentang aktivitas database yang berpotensi tidak biasa, lihatAnomali berbasis aktivitas data RDS.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk database terkait, disarankan untuk segera mengubah kata sandi pengguna database terkait dan mencabut aksesnya. Tinjau log audit yang tersedia untuk menentukan ruang lingkup data yang dihapus, dan memulai pemulihan point-in-time dari pencadangan otomatis jika kehilangan data dikonfirmasi. Juga disarankan untuk menempatkan database di VPC pribadi dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan aktivitas destruktif anomali.

Exfiltration:RDS/MaliciousIPCaller

Alamat IP yang dikaitkan dengan aktivitas berbahaya yang diketahui mengeksekusi kueri ekstraksi data pada database RDS di akun Anda.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas RDS DB

Temuan ini memberi tahu Anda bahwa alamat IP yang terkait dengan aktivitas berbahaya yang diketahui mengeksekusi kueri basis data yang konsisten dengan eksfiltrasi data pada database RDS di lingkungan Anda. AWS Ini menunjukkan bahwa pengguna dan kata sandi yang terkait

dengan database RDS di akun Anda mungkin telah disusupi, dan data database RDS mungkin telah diekstraksi oleh aktor yang berpotensi jahat.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, hal tersebut mungkin menandakan bahwa kredensial pengguna telah terekspos atau disusupi. Disarankan untuk mengubah kata sandi pengguna database terkait, dan meninjau log data RDS yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang disusupi. Disarankan untuk mengidentifikasi data yang dapat diakses oleh pengguna yang terkena dampak dan menilai dampak bisnis dari setiap data yang berpotensi diekstraksi. Juga disarankan untuk menempatkan database di VPC pribadi dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan aktivitas eksfiltrasi anomali.

Exfiltration:RDS/TorIPCaller

Alamat IP node keluar Tor mengeksekusi kueri ekstraksi data pada database RDS di akun Anda.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas RDS DB

Temuan ini memberi tahu Anda bahwa alamat IP node keluar Tor mengeksekusi kueri database yang konsisten dengan eksfiltrasi data pada database RDS di lingkungan Anda. AWS Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Simpul Tor terakhir disebut sebagai simpul keluar. Ini dapat menunjukkan akses tidak sah ke sumber daya RDS di akun Anda, dengan maksud menyembunyikan identitas asli pengguna anonim saat mengekstraksi data.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, hal tersebut mungkin menandakan bahwa kredensial pengguna telah terekspos atau disusupi. Disarankan untuk mengubah kata sandi pengguna database terkait, dan meninjau log data RDS yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang disusupi. Disarankan untuk mengidentifikasi data yang dapat diakses oleh pengguna yang terkena dampak dan menilai dampak bisnis dari setiap data yang berpotensi diekstraksi. Juga disarankan untuk menempatkan database di VPC pribadi dan membatasi aturan

grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan aktivitas eksfiltrasi anomali.

Impact:RDS/MaliciousIPCaller

Alamat IP yang dikaitkan dengan aktivitas berbahaya yang diketahui mengeksekusi pernyataan destruktif pada database RDS di akun Anda.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas RDS DB

Temuan ini memberi tahu Anda bahwa alamat IP yang terkait dengan aktivitas berbahaya yang diketahui mengeksekusi pernyataan database dengan dampak destruktif pada database RDS di lingkungan Anda. AWS Ini menunjukkan bahwa pengguna dan kata sandi yang terkait dengan database RDS di akun Anda mungkin telah disusupi, dan database RDS mungkin telah mengalami operasi destruktif oleh aktor yang berpotensi jahat.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, hal tersebut mungkin menandakan bahwa kredensial pengguna telah terekspos atau disusupi. Disarankan untuk segera mengubah kata sandi pengguna database terkait dan mencabut akses mereka. Tinjau log data RDS yang tersedia untuk menentukan ruang lingkup operasi destruktif yang dilakukan, dan memulai pemulihan dari cadangan jika perlu. Juga disarankan untuk menempatkan database di VPC pribadi dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Memulihkan database yang berpotensi dikompromikan dengan aktivitas destruktif anomali.

Impact:RDS/TorIPCaller

Alamat IP node keluar Tor mengeksekusi pernyataan destruktif pada database RDS di akun Anda.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas RDS DB

Temuan ini memberi tahu Anda bahwa alamat IP node keluar Tor mengeksekusi pernyataan database dengan dampak destruktif pada database RDS di lingkungan Anda. AWS Tor adalah jaringan overlay untuk memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Simpul Tor terakhir disebut sebagai simpul keluar. Ini dapat menunjukkan akses tidak sah ke sumber daya RDS di akun Anda, dengan maksud menyembunyikan identitas asli pengguna anonim saat melakukan operasi destruktif.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk basis data terkait, hal tersebut mungkin menandakan bahwa kredensial pengguna telah terekspos atau disusupi. Disarankan untuk segera mengubah kata sandi pengguna database terkait dan mencabut akses mereka. Tinjau log data RDS yang tersedia untuk menentukan ruang lingkup operasi destruktif yang dilakukan, dan memulai pemulihan dari cadangan jika perlu. Juga disarankan untuk menempatkan database di VPC pribadi dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Lihat informasi yang lebih lengkap di Memulihkan database yang berpotensi dikompromikan dengan aktivitas destruktif anomali.

Jenis temuan Perlindungan Lambda

Bagian ini menjelaskan jenis temuan yang spesifik untuk AWS Lambda sumber daya Anda dan memiliki yang `resourceType` terdaftar sebagai`Lambda`. Untuk semua temuan Lambda, kami sarankan Anda memeriksa sumber daya yang dimaksud dan menentukan apakah itu berperilaku dengan cara yang diharapkan. Jika aktivitas diotorisasi, Anda dapat menggunakan aturan Suppression atau IP Tepercaya dan daftar ancaman untuk mencegah pemberitahuan positif palsu untuk sumber daya tersebut.

Jika aktivitasnya tidak terduga, praktik terbaik keamanan adalah mengasumsikan bahwa Lambda berpotensi dikompromikan dan mengikuti rekomendasi remediasi.

Topik

- Backdoor:Lambda/C&CActivity.B
- CryptoCurrency:Lambda/BitcoinTool.B
- Trojan:Lambda/BlackholeTraffic
- Trojan:Lambda/DropPoint
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- UnauthorizedAccess:Lambda/TorClient

- UnauthorizedAccess:Lambda/TorRelay

Backdoor:Lambda/C&CActivity.B

Fungsi Lambda adalah menanyakan alamat IP yang dikaitkan dengan server perintah dan kontrol yang dikenal.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda yang terdaftar di lingkungan AWS Anda sedang menanyakan alamat IP yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. Fungsi Lambda yang terkait dengan temuan yang dihasilkan berpotensi dikompromikan. Server C&C adalah komputer yang mengeluarkan perintah kepada anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet, yang mungkin termasuk PC, server, perangkat seluler, dan perangkat Internet of Things, yang terinfeksi dan dikendalikan oleh jenis malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disusupi, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet, server C&C mungkin juga mengeluarkan perintah untuk memulai penolakan layanan terdistribusi.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki fungsi Lambda yang berpotensi dikompromikan.

CryptoCurrency:Lambda/BitcoinTool.B

Fungsi Lambda adalah menanyakan alamat IP yang terkait dengan aktivitas terkait cryptocurrency.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda yang terdaftar di lingkungan AWS Anda menanyakan alamat IP yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Aktor

ancaman mungkin berusaha untuk mengambil kendali atas fungsi Lambda untuk menggunakannya kembali dengan jahat untuk penambangan cryptocurrency yang tidak sah.

Rekomendasi remediasi:

Jika Anda menggunakan fungsi Lambda ini untuk menambang atau mengelola mata uang kripto, atau fungsi ini terlibat dalam aktivitas blockchain, ancaman ini berpotensi terjadi di lingkungan Anda. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut jenis temuan dengan nilai CryptoCurrency:Lambda/BitcoinTool.B. Kriteria filter kedua adalah nama fungsi Lambda dari fungsi yang terlibat dalam aktivitas blockchain. Untuk informasi tentang membuat aturan penekanan, lihat Aturan penekanan.

Jika aktivitas ini tidak terduga, fungsi Lambda berpotensi disusupi. Untuk informasi selengkapnya, lihat Memperbaiki fungsi Lambda yang berpotensi dikompromikan.

Trojan:Lambda/BlackholeTraffic

Fungsi Lambda mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang merupakan lubang hitam yang dikenal.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda yang terdaftar di lingkungan AWS Anda mencoba berkomunikasi dengan alamat IP lubang hitam (atau lubang wastafel). Black hole adalah tempat di jaringan di mana lalu lintas yang masuk atau keluar diam-diam dibuang tanpa menginformasikan sumber bahwa datanya tidak sampai ke penerima yang dimaksudkan. Alamat IP black hole menentukan mesin host yang tidak berjalan atau alamat yang tidak memiliki host yang ditetapkan. Fungsi Lambda yang terdaftar berpotensi dikompromikan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki fungsi Lambda yang berpotensi dikompromikan.

Trojan:Lambda/DropPoint

Fungsi Lambda mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang diketahui memiliki kredensi dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda yang terdaftar di lingkungan AWS Anda mencoba berkomunikasi dengan alamat IP host jarak jauh yang diketahui menyimpan kredensil dan data curian lainnya yang ditangkap oleh malware.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki fungsi Lambda yang berpotensi dikompromikan.

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Fungsi Lambda membuat koneksi ke alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Medium

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda di lingkungan AWS Anda berkomunikasi dengan alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Dalam GuardDuty, daftar ancaman terdiri dari alamat IP berbahaya yang diketahui. GuardDuty menghasilkan temuan berdasarkan daftar ancaman yang diunggah. Anda dapat melihat detail daftar ancaman di detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki fungsi Lambda yang berpotensi dikompromikan.

UnauthorizedAccess:Lambda/TorClient

Fungsi Lambda adalah membuat koneksi ke Tor Guard atau node Authority.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda di lingkungan AWS Anda membuat koneksi ke Tor Guard atau node Otoritas. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Simpul Tor Guard dan Authority bertindak sebagai gateway awal ke dalam jaringan Tor. Lalu lintas ini dapat menunjukkan bahwa fungsi Lambda ini berpotensi dikompromikan. Sekarang bertindak sebagai klien di jaringan Tor.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki fungsi Lambda yang berpotensi dikompromikan.

UnauthorizedAccess:Lambda/TorRelay

Fungsi Lambda adalah membuat koneksi ke jaringan Tor sebagai relay Tor.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda di lingkungan AWS Anda membuat koneksi ke jaringan Tor dengan cara yang menunjukkan bahwa itu bertindak sebagai relai Tor. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Tor memungkinkan komunikasi anonim dengan meneruskan lalu lintas berpotensi ilegal klien dari satu relay Tor ke yang lain.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Lihat informasi yang lebih lengkap di Memperbaiki fungsi Lambda yang berpotensi dikompromikan.

GuardDuty Jenis penemuan Perlindungan AI

Saat Anda mengaktifkan Perlindungan AI, GuardDuty menganalisis peristiwa AWS CloudTrail manajemen dan peristiwa data dari Amazon Bedrock dan Amazon SageMaker AI. GuardDuty menggunakan data ini untuk mendeteksi aktivitas yang berpotensi mencurigakan yang menargetkan beban kerja AI Anda. Ketika GuardDuty mendeteksi ancaman potensial, itu menghasilkan salah satu jenis temuan berikut. Untuk `Resource type` temuan ini adalah`AccessKey`, dan temuan tersebut mengidentifikasi identitas IAM yang menggunakan model.

Setiap temuan juga mencakup detail tentang sumber daya AI yang terpengaruh dalam `resource` objek temuan. Impact:IAMUser/CostHarvestingTemuan Impact:IAMUser/AnomalousModelInvocation dan termasuk `resource.modelDetails` daftar yang mengidentifikasi model Amazon Bedrock atau Amazon SageMaker AI yang dipanggil. Tem Impact:IAMUser/PromptInjection.Direct uan tersebut mencakup `resource.bedrockGuardrailDetails` objek yang menggambarkan Amazon Bedrock Guardrail yang melakukan intervensi. Anda dapat melihat detail ini di GuardDuty konsol atau di JSON pencarian.

Jenis Impact:IAMUser/AnomalousModelInvocation dan Impact:IAMUser/CostHarvesting temuan berlaku untuk pemanggilan model Amazon Bedrock dan Amazon SageMaker AI. Jenis tem Impact:IAMUser/PromptInjection.Direct uan berlaku untuk beban kerja Amazon Bedrock yang menggunakan Amazon Bedrock Guardrails.

Topik

- Impact:IAMUser/AnomalousModelInvocation
- Impact:IAMUser/CostHarvesting
- Impact:IAMUser/PromptInjection.Direct

Impact:IAMUser/AnomalousModelInvocation

Identitas IAM memanggil model Amazon Bedrock atau Amazon SageMaker AI dengan cara yang menyimpang dari baseline yang ditetapkan untuk identitas atau akun.

Tingkat keparahan default: Rendah

- Fitur: Per lindungan AI

Temuan ini memberi tahu Anda bahwa identitas IAM memanggil model Amazon Bedrock atau Amazon SageMaker AI dengan cara yang menyimpang dari aktivitas historis identitas atau akun. Aktivitas ini mungkin menunjukkan bahwa aktor ancaman menggunakan kredenSIAL yang dikompromikan untuk mengakses model dasar di akun Anda. Misalnya, aktor mungkin menyelidiki model, membuat input permusuhan, atau menjalankan permintaan otomatis.

GuardDuty menetapkan dasar aktivitas pemanggilan model normal untuk setiap identitas IAM dan Akun AWS yang memanggil Amazon Bedrock atau Amazon AI. SageMaker GuardDuty fitur profil aktivitas pemanggilan, termasuk yang berikut:

- API pemanggilan model yang dipanggil identitas
- Model yang dipanggil identitas
- Alamat IP sumber dan organisasi Nomor Sistem Otonom (ASN) yang terkait
- Agen pengguna yang membuat permintaan

Ketika GuardDuty mengamati aktivitas yang menyimpang secara signifikan dari baseline ini, itu menghasilkan temuan ini. Contohnya termasuk pemanggilan dari alamat IP yang sebelumnya tidak terlihat, agen pengguna yang sebelumnya tidak terlihat, atau model yang tidak pernah dipanggil identitas. Temuan ini mencakup `resource.modelDetails` daftar yang mengidentifikasi model yang terlibat dalam aktivitas mencurigakan. Setiap entri berisi model dasar Amazon Bedrock yang `modelId` mewakili, profil inferensi, model yang disediakan, khusus, atau diimpor ARN, titik akhir Amazon Bedrock Marketplace, sumber daya prompt, atau nama titik akhir Amazon SageMaker AI.

Temuan ini memetakan teknik MITRE ATLAS AML.T0040 - Akses API Inferensi Model AI di situs web MITRE ATLAS.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Untuk mengurangi risiko pemanggilan model yang tidak sah, batasi identitas mana yang dapat memanggil model. Cakupan akses ke API pemanggilan model berikut hanya ke prinsipal dan model yang memerlukannya:

- `bedrock:InvokeModel`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:Converse`

- `bedrock:ConverseStream`
- `bedrock-mantle:CreateInference`
- `sagemaker:InvokeEndpoint`
- `sagemaker:InvokeEndpointAsync`
- `sagemaker:InvokeEndpointWithResponseStream`

Untuk menolak inferensi model di seluruh organisasi Anda yang tidak diperlukan, Anda dapat menggunakan kebijakan kontrol layanan (SCP). Untuk informasi selengkapnya, lihat contoh Identity-based kebijakan untuk Amazon Bedrock di Panduan Pengguna Amazon Bedrock dan contoh kebijakan berbasis SageMaker identitas Amazon AI di Panduan Pengembang AI Amazon SageMaker .

Impact:IAMUser/CostHarvesting

Identitas IAM menggunakan model Amazon Bedrock atau Amazon SageMaker AI dengan volume token anomali yang mungkin mengindikasikan serangan biaya panen.

Tingkat keparahan default: Rendah

- Fitur: Per lindungan AI

Temuan ini memberi tahu Anda bahwa identitas IAM memanggil model Amazon Bedrock atau Amazon SageMaker AI dengan volume token input atau output yang menyimpang secara signifikan dari baseline untuk identitas atau akun. Dalam serangan pemanenan biaya, pelaku ancaman mengirimkan input yang mahal dari segi komputasi ke model untuk meningkatkan biaya operasi beban kerja AI, tanpa harus melakukan eksfiltrasi data. Input ini mungkin mencakup prompt yang terlalu panjang atau sengaja dibuat salah bentuk.

GuardDuty menetapkan garis dasar volume token input rata-rata dan volume token keluaran rata-rata untuk setiap identitas dan akun IAM yang memanggil model Amazon Bedrock atau Amazon AI. SageMaker Ketika GuardDuty mengamati pemanggilan dengan jumlah token yang melebihi garis dasar ini, dan mengkorelasikan anomali volume dengan sinyal tidak biasa lainnya, GuardDuty menghasilkan temuan ini. Temuan tersebut melaporkan aktivitas anomali dalam `service.detection` objek, termasuk pemanggilan yang diamati dan volume token yang menyimpang dari garis dasar. Ini juga termasuk `resource.modelDetails` daftar yang mengidentifikasi model yang ditargetkan. Setiap entri berisi model dasar Amazon Bedrock yang

`modelId` mewakili, profil inferensi, model yang disediakan, khusus, atau diimpor ARN, titik akhir Amazon Bedrock Marketplace, sumber daya prompt, atau nama titik akhir Amazon SageMaker AI.

Temuan ini memetakan teknik MITRE ATLAS AML.T0034 - Cost Harvesting di situs web MITRE ATLAS.

Rekomendasi perbaikan:

Jika aktivitas ini tidak terduga untuk identitas terkait, kredensialnya mungkin telah dikompromikan dan digunakan untuk menaikkan biaya beban kerja AI Anda. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials. Tinjau pemanggilan model yang terkait dengan identitas, dan batasi akses ke model yang terpengaruh dengan mencakupi akses ke API pemanggilan model berikut hanya untuk prinsipal yang memerlukannya:

- `bedrock:InvokeModel`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:Converse`
- `bedrock:ConverseStream`
- `bedrock-mantle:CreateInference`
- `sagemaker:InvokeEndpoint`
- `sagemaker:InvokeEndpointAsync`
- `sagemaker:InvokeEndpointWithResponseStream`

Untuk mendeteksi dan menahan pengeluaran abnormal, Anda dapat menggunakan Ang AWS garan, termasuk tindakan anggaran yang menerapkan kebijakan IAM yang membatasi saat ambang anggaran terlampaui, dan Det eksi Anomali AWS Biaya. Untuk mengaitkan biaya Amazon Bedrock ke beban kerja tertentu, Anda dapat melampirkan tag alokasi biaya ke profil infer ensi aplikasi.

Impact:IAMUser/PromptInjection.Direct

Amazon Bedrock Guardrail mendeteksi upaya injeksi prompt langsung dalam invokasi yang dibuat oleh identitas IAM.

Tingkat keparahan default: Rendah

- Fitur: Per lindungan AI

Temuan ini memberi tahu Anda bahwa Amazon Bedrock Guardrail yang dikonfigurasi untuk beban kerja Amazon Bedrock di akun Anda mendeteksi upaya injeksi prompt langsung. Dalam serangan injeksi prompt langsung, aktor ancaman membuat prompt jahat sebagai masukan ke model dasar. Prompt membuat model mengabaikan instruksi aslinya dan mengikuti instruksi penyerang sebagai gantinya. Injeksi prompt dapat memberikan akses awal kepada penyerang untuk melakukan langkah-langkah tambahan terhadap aplikasi AI, seperti melakukan eksfiltrasi data, memanggil alat yang tidak sah, atau melewati kontrol keamanan.

GuardDuty menghasilkan temuan ini ketika Amazon Bedrock Guardrail melakukan intervensi pada pemanggilan karena mendeteksi serangan cepat dengan keyakinan tinggi. GuardDuty Untuk mengaktifkan deteksi injeksi prompt langsung, konfigurasikan Amazon Bedrock Guardrail dengan filter konten serangan cepat. Untuk memastikan pagar pembatas mengevaluasi pemanggilan di seluruh lingkungan Anda, terapkan secara luas alih-alih mengandalkan aplikasi individual untuk melampirkannya ke setiap permintaan. Anda dapat menerapkan pagar pembatas untuk semua pemanggilan model Amazon Bedrock di akun, atau di seluruh organisasi Anda dengan menggunakan kebijakan Amazon Bedrock di. AWS Organizations Untuk informasi selengkapnya, lihat M enerapkan perlindungan lintas akun dengan penegakan Amazon Bedrock Guardrails di Panduan Pengguna Amazon Bedrock. Ketika pagar pembatas mengevaluasi pemanggilan, Amazon Bedrock mencatat evaluasi dalam peristiwa AWS CloudTrail data, yang GuardDuty menganalisis untuk menghasilkan temuan ini. Jika pagar pembatas juga menerapkan filter informasi sensitif ketika mengevaluasi pemanggilan, temuan tersebut mencakup detail tentang jenis informasi sensitif yang terdeteksi.

Temuan tersebut mencakup objek `resource.bedrockGuardrailDetails` yang menggambarkan batasan pengaman yang mengintervensi. Tabel berikut menjelaskan bidang dalam objek ini.

Bidang	Deskripsi
`guardrails`	Daftar pagar pembatas yang mengevaluasi pemanggilan. Setiap entri menyertakan Nama Sumber Daya Amazon (`arn`) dan pag `version` ar pembatas. Beberapa pagar pembatas dapat muncul ketika pagar pembatas yang ditegakkan oleh akun atau organisasi dan pagar pembatas tingkat permintaan mengevaluasi pemanggilan yang sama.
`guardrailAction`	Tindakan yang diambil pagar pembatas. GuardDuty menghasilkan temuan ini ketika nilainya ada`GUARDRAIL_INTERVENED` .

Bidang	Deskripsi
`guardrailSource`	Konten yang dievaluasi pagar pembatas. `INPUT`menunjukkan prompt yang dikirim ke model, dan `OUTPUT` menunjukkan respons dari model.
`contentPolicyFilters`	Daftar filter kebijakan konten yang diterapkan pagar pembatas. Untuk jenis temuan ini, entr `type` i memiliki `PROMPT_ATTACK` a dan `confidence` ofHIGH. Ini `action` adalah `BLOCKED` jika pagar pembatas memblokir konten, atau `NONE` jika pagar pembatas mendeteksi serangan prompt tetapi dikonfigurasi hanya untuk melaporkannya.
`sensitiveInformationFilters`	Filter informasi sensitif yang diterapkan pagar pembatas saat mengevaluasi pemanggilan. Setiap entri memiliki a `type` yang mengidentifikasi jenis informasi sensitif yang dideteksi pagar pembatas, seperti `AWS_SECRET_KEY` atau`PASSWORD`, dan apakah pagar pem `action` batas memblokir konten, `BLOCKED` jika pagar pembatas menutupinya, atau `ANONYMIZED` `NONE` jika pagar pembatas mendeteksinya tetapi dikonfigurasi hanya untuk melaporkannya. Temuan mencatat jenis informasi yang terdeteksi, bukan konten itu sendiri.

Temuan ini memetakan teknik MITRE ATLAS AML.T0051 - LLM Prompt Injection di situs web MITRE ATLAS.

Rekomendasi perbaikan:

Tinjau prompt yang memicu intervensi pagar pembatas dan identitas IAM yang mengirimkan prompt. Jika aktivitas tidak terduga untuk identitas terkait, kredensialnya mungkin telah dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials. Jika pagar pembatas mendeteksi tetapi tidak memblokir serangan prompt, pertimbangkan untuk mengatur tindakan filter konten serangan prompt ke Blokir daripada Deteksi sehingga pagar pembatas memblokir konten. Untuk informasi selengkapnya, lihat Opsi untuk menangani konten berbahaya yang terdeteksi oleh Amazon Bedrock Guardrails di Panduan Pengguna Amazon Bedrock. Anda juga dapat membatasi akses ke API pemanggilan Amazon Bedrock untuk identitas yang terpengaruh.

Tipe temuan yang sudah dihentikan

Temuan adalah pemberitahuan yang berisi rincian tentang potensi masalah keamanan yang GuardDuty ditemukan. Untuk informasi tentang perubahan penting pada jenis GuardDuty temuan, termasuk jenis temuan yang baru ditambahkan atau yang sudah pensiun, lihatRiwayat dokumen untuk Amazon GuardDuty.

Jenis temuan berikut sudah pensiun dan tidak lagi dihasilkan oleh GuardDuty.

> **Important**
>
> Anda tidak dapat mengaktifkan kembali tipe GuardDuty temuan yang sudah pensiun.

Topik

- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Exfiltration:S3/ObjectRead.Unusual
- Impact:S3/PermissionsModification.Unusual
- Impact:S3/ObjectDelete.Unusual
- Discovery:S3/BucketEnumeration.Unusual
- Persistence:IAMUser/NetworkPermissions
- Persistence:IAMUser/ResourcePermissions
- Persistence:IAMUser/UserPermissions
- PrivilegeEscalation:IAMUser/AdministrativePermissions
- Recon:IAMUser/NetworkPermissions
- Recon:IAMUser/ResourcePermissions
- Recon:IAMUser/UserPermissions
- ResourceConsumption:IAMUser/ComputeResources
- Stealth:IAMUser/LoggingConfigurationModified
- UnauthorizedAccess:IAMUser/ConsoleLogin
- UnauthorizedAccess:EC2/TorIPCaller

- Backdoor:EC2/XORDDOS
- Behavior:IAMUser/InstanceLaunchUnusual
- CryptoCurrency:EC2/BitcoinTool.A
- UnauthorizedAccess:IAMUser/UnusualASNCaller

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Kontainer istimewa dengan akses tingkat root diluncurkan di klaster Kubernetes Anda.

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa sebuah kontainer yang diluncurkan pada klaster Kubernetes Anda menggunakan citra yang belum pernah digunakan untuk meluncurkan kontainer berhak akses di klaster Anda. Sebuah kontainer berhak akses memiliki akses tingkat root ke host. Penyerang dapat meluncurkan kontainer berhak akses sebagai taktik eskalasi hak akses untuk mendapatkan akses ke dan kemudian menyusupi host.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan kontainer mungkin disusupi. Cabut akses pengguna dan pulihkan perubahan yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Persistence:Kubernetes/ContainerWithSensitiveMount

Sebuah kontainer diluncurkan dengan jalur host eksternal sensitif yang dipasang di dalamnya.

Tingkat keparahan default: Medium

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa wadah diluncurkan dengan konfigurasi yang menyertakan jalur host sensitif dengan akses tulis di `volumeMounts` bagian tersebut. Ini membuat jalur host

sensitif dapat diakses dan dapat ditulis dari dalam wadah. Teknik ini biasanya digunakan oleh penyerang untuk mendapatkan akses ke sistem file host.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan kontainer mungkin disusupi. Cabut akses pengguna dan pulihkan perubahan yang dilakukan oleh penyerang pada klaster Anda. Untuk informasi selengkapnya, lihat Memperbaiki temuan Perlindungan EKS.

Jika peluncuran kontainer ini memang diharapkan, gunakan aturan penekanan yang terdiri dari kriteria filter berdasarkan bidang `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Dalam kriteria filter, bidang `imagePrefix` harus sama dengan `imagePrefix` yang ditentukan dalam temuan tersebut. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat Aturan penekanan.

Exfiltration:S3/ObjectRead.Unusual

Entitas IAM memanggil API S3 dengan cara yang mencurigakan.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM di AWS lingkungan Anda melakukan panggilan API yang melibatkan bucket S3 dan yang berbeda dari baseline yang ditetapkan entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini dikaitkan dengan tahap eksfiltrasi serangan, ketika penyerang sedang mencoba mengumpulkan data. Aktivitas ini mencurigakan karena cara entitas IAM memanggil API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat invokasi tipe API ini, atau API diinvokasi dari lokasi yang tidak biasa.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Impact:S3/PermissionsModification.Unusual

Entitas IAM menginvokasi API untuk mengubah izin pada satu sumber daya S3 atau lebih.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini memberi tahu Anda bahwa entitas IAM membuat panggilan API yang dirancang untuk mengubah izin pada satu atau lebih bucket atau objek di lingkungan AWS Anda. Tindakan ini dapat dilakukan oleh penyerang untuk memungkinkan informasi dibagikan di luar akun. Aktivitas ini mencurigakan karena cara entitas IAM memanggil API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat invokasi tipe API ini, atau API diinvokasi dari lokasi yang tidak biasa.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Impact:S3/ObjectDelete.Unusual

Entitas IAM menginvokasi API yang digunakan untuk menghapus data dalam bucket S.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini memberi tahu Anda bahwa entitas IAM tertentu di AWS lingkungan Anda membuat panggilan API yang dirancang untuk menghapus data di bucket S3 yang terdaftar dengan menghapus bucket itu sendiri. Aktivitas ini mencurigakan karena cara entitas IAM menginvokasi API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat invokasi tipe API ini, atau API diinvokasi dari lokasi yang tidak biasa.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Discovery:S3/BucketEnumeration.Unusual

Entitas IAM menginvokasi API S3 yang digunakan untuk menemukan bucket S3 dalam jaringan Anda.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini memberi tahu Anda bahwa entitas IAM telah menginvokasi API S3 untuk menemukan bucket S3 dalam lingkungan Anda, seperti `ListBuckets`. Jenis aktivitas ini dikaitkan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah AWS lingkungan Anda rentan terhadap serangan yang lebih luas. Aktivitas ini mencurigakan karena cara entitas IAM menginvokasi API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat invokasi tipe API ini, atau API diinvokasi dari lokasi yang tidak biasa.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk principal terkait, hal tersebut mungkin mengindikasikan kredensialnya telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat Memperbaiki bucket S3 yang berpotensi dikompromikan.

Persistence:IAMUser/NetworkPermissions

Entitas IAM memanggil API yang biasa digunakan untuk mengubah izin akses jaringan untuk grup keamanan, rute, dan ACL di AWS akun.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menunjukkan bahwa prinsipal tertentu (Pengguna root akun AWS, peran IAM, atau pengguna) di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Principal ini sebelumnya tidak memiliki riwayat invokasi API ini.

Temuan ini dipicu ketika pengaturan konfigurasi jaringan berubah dalam keadaan yang mencurigakan, seperti ketika prinsipal memanggil API `CreateSecurityGroup` tanpa riwayat sebelumnya. Penyerang sering mencoba untuk mengubah grup keamanan untuk memungkinkan lalu lintas masuk tertentu pada berbagai port untuk meningkatkan kemampuannya untuk mengakses instans EC2.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Persistence:IAMUser/ResourcePermissions

Seorang prinsipal memanggil API yang biasa digunakan untuk mengubah kebijakan akses keamanan berbagai sumber daya di Akun AWS.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API yang dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menunjukkan bahwa prinsipal tertentu (Pengguna root akun AWS, peran IAM, atau pengguna) di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Principal ini sebelumnya tidak memiliki riwayat invokasi API ini.

Temuan ini dipicu ketika perubahan terdeteksi pada kebijakan atau izin yang dilampirkan ke AWS sumber daya, seperti ketika prinsipal di AWS lingkungan Anda memanggil `PutBucketPolicy` API tanpa riwayat sebelumnya untuk melakukannya. Beberapa layanan, seperti Amazon S3, mendukung izin yang melekat pada sumber daya yang memberikan satu akses utama atau lebih ke sumber daya. Dengan kredensial curian, penyerang dapat mengubah kebijakan yang melekat pada sumber daya untuk memperoleh akses ke sumber daya tersebut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Persistence:IAMUser/UserPermissions

Prinsipal memanggil API yang biasa digunakan untuk menambah, memodifikasi, atau menghapus pengguna, grup, atau kebijakan IAM di AWS akun.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menunjukkan bahwa prinsipal tertentu (Pengguna root akun AWS, peran IAM, atau pengguna) di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Principal ini sebelumnya tidak memiliki riwayat invokasi API ini.

Temuan ini dipicu oleh perubahan mencurigakan pada izin terkait pengguna di AWS lingkungan Anda, seperti saat prinsipal di AWS lingkungan Anda memanggil `AttachUserPolicy` API tanpa riwayat sebelumnya untuk melakukannya. Penyerang dapat menggunakan kredensial curian untuk membuat pengguna baru, menambahkan kebijakan akses ke pengguna yang ada, atau membuat kunci akses untuk memaksimalkan akses mereka ke akun, bahkan jika titik akses asli mereka ditutup. Misalnya, pemilik akun mungkin memperhatikan bahwa pengguna atau kata sandi IAM tertentu telah dicuri dan menghapusnya dari akun. Namun, mereka mungkin tidak menghapus pengguna lain yang dibuat oleh kepala admin yang dibuat secara curang, sehingga AWS akun mereka dapat diakses oleh penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

PrivilegeEscalation:IAMUser/AdministrativePermissions

Principal telah mencoba menetapkan kebijakan yang sangat permisif untuk diri mereka sendiri.

Tingkat keparahan default: Rendah*

> **Note**
>
> Tingkat kepelikan temuan ini Rendah jika upaya eskalasi hak istimewa tidak berhasil, dan Medium jika upaya eskalasi hak istimewa berhasil.

Temuan ini menunjukkan bahwa entitas IAM tertentu di AWS lingkungan Anda menunjukkan perilaku yang dapat menjadi indikasi serangan eskalasi hak istimewa. Temuan ini dipicu ketika pengguna atau IAM role mencoba untuk menetapkan kebijakan yang sangat permisif untuk diri mereka sendiri. Jika pengguna atau peran yang dimaksud tidak dimaksudkan untuk memiliki hak administratif, kredensial pengguna dapat disusupi atau izin peran mungkin tidak dikonfigurasi dengan benar.

Penyerang akan menggunakan kredensial curian untuk membuat pengguna baru, menambahkan kebijakan akses ke pengguna yang ada, atau membuat kunci akses untuk memaksimalkan akses mereka ke akun bahkan jika titik akses asli mereka ditutup. Misalnya, pemilik akun mungkin memperhatikan bahwa kredensi masuk pengguna IAM tertentu dicuri dan dihapus dari akun, tetapi mungkin tidak menghapus pengguna lain yang dibuat oleh kepala admin yang dibuat secara curang, sehingga AWS akun mereka masih dapat diakses oleh penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Recon:IAMUser/NetworkPermissions

Prinsipal memanggil API yang biasa digunakan untuk mengubah izin akses jaringan untuk grup keamanan, rute, dan ACL di AWS akun.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menunjukkan bahwa prinsipal tertentu (Pengguna root akun AWS, peran IAM, atau pengguna) di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Principal ini sebelumnya tidak memiliki riwayat invokasi API ini.

Temuan ini dipicu ketika izin akses sumber daya di akun AWS Anda diperiksa dalam keadaan yang mencurigakan. Misalnya, jika prinsipal memanggil API `DescribeInstances` tanpa riwayat

sebelumnya. Seorang penyerang mungkin menggunakan kredensyal curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensyal yang lebih berharga atau menentukan kemampuan kredensyal yang sudah mereka miliki.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Recon:IAMUser/ResourcePermissions

Seorang prinsipal memanggil API yang biasa digunakan untuk mengubah kebijakan akses keamanan berbagai sumber daya di AWS akun.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menunjukkan bahwa prinsipal tertentu (Pengguna root akun AWS, peran IAM, atau pengguna) di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Principal ini sebelumnya tidak memiliki riwayat invokasi API ini.

Temuan ini dipicu ketika izin akses sumber daya di akun AWS Anda diperiksa dalam keadaan yang mencurigakan. Misalnya, jika prinsipal memanggil API `DescribeInstances` tanpa riwayat sebelumnya. Seorang penyerang mungkin menggunakan kredensyal curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensyal yang lebih berharga atau menentukan kemampuan kredensyal yang sudah mereka miliki.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Recon:IAMUser/UserPermissions

Prinsipal memanggil API yang biasa digunakan untuk menambah, memodifikasi, atau menghapus pengguna, grup, atau kebijakan IAM di AWS akun.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini dipicu ketika izin pengguna di AWS lingkungan Anda diselidiki dalam keadaan yang mencurigakan. Misalnya, jika prinsipal (Pengguna root akun AWS, peran IAM, atau pengguna IAM) memanggil `ListInstanceProfilesForRole` API tanpa riwayat sebelumnya untuk melakukannya. Seorang penyerang mungkin menggunakan kredensyal curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensyal yang lebih berharga atau menentukan kemampuan kredensyal yang sudah mereka miliki.

Temuan ini menunjukkan bahwa prinsip tertentu di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Principal ini sebelumnya tidak memiliki riwayat invokasi API ini dengan cara ini.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

ResourceConsumption:IAMUser/ComputeResources

Principal menginvokasi API yang biasa digunakan untuk meluncurkan sumber daya komputasi seperti instans EC2.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini dipicu ketika instans EC2 di akun yang tercantum dalam lingkungan AWS Anda diluncurkan dalam keadaan yang mencurigakan. Temuan ini menunjukkan bahwa prinsip tertentu di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan; misalnya, jika prinsipal (, peran IAM Pengguna root akun AWS, atau pengguna IAM) memanggil `RunInstances` API tanpa riwayat sebelumnya untuk melakukannya. Hal ini mungkin merupakan indikasi penyerang menggunakan kredensial curian untuk mencuri waktu komputasi (mungkin untuk penambangan mata uang kripto atau peretasan kata sandi). Ini juga bisa menjadi indikasi penyerang menggunakan instans EC2 di AWS lingkungan Anda dan kredensialnya untuk mempertahankan akses ke akun Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

Stealth:IAMUser/LoggingConfigurationModified

Prinsipal memanggil API yang biasa digunakan untuk menghentikan CloudTrail Logging, menghapus log yang ada, dan menghilangkan jejak aktivitas di AWS akun.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini dipicu ketika konfigurasi pencatatan log di akun AWS yang tercantum dalam lingkungan Anda diubah dalam keadaan yang mencurigakan. Temuan ini memberi tahu Anda bahwa prinsip

tertentu di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan; misalnya, jika prinsipal (, peran IAM Pengguna root akun AWS, atau pengguna IAM) memanggil API tanpa riwayat sebelumnya untuk melakukannya. `StopLogging` Hal ini bisa menjadi indikasi penyerang yang mencoba menutupi jejak mereka dengan menghilangkan jejak aktivitas mereka.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

UnauthorizedAccess:IAMUser/ConsoleLogin

Login konsol yang tidak biasa oleh kepala sekolah di Anda AWS akun diamati.

Tingkat keparahan default: Sedang*

> **Note**
>
> Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensyal sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini dipicu ketika login konsol terdeteksi dalam keadaan yang mencurigakan. Misalnya, jika prinsipal tanpa riwayat sebelumnya untuk melakukannya, memanggil ConsoleLogin API dari klien yang belum pernah digunakan sebelumnya atau lokasi yang tidak biasa. Ini bisa menjadi indikasi kredensyal curian yang digunakan untuk mendapatkan akses ke AWS akun Anda, atau pengguna yang valid mengakses akun dengan cara yang tidak valid atau kurang aman (misalnya, tidak melalui VPN yang disetujui).

Temuan ini memberi tahu Anda bahwa prinsip tertentu di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Principal ini tidak memiliki riwayat aktivitas login sebelumnya menggunakan aplikasi klien ini dari lokasi spesifik ini.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

UnauthorizedAccess:EC2/TorIPCaller

Instans EC2 Anda menerima koneksi masuk dari simpul keluar Tor.

Tingkat keparahan default: Medium

Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda menerima koneksi masuk dari node keluar Tor. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Hal ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relai antara serangkaian simpul jaringan. Simpul Tor terakhir disebut sebagai simpul keluar. Temuan ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Backdoor:EC2/XORDDOS

Instans EC2 mencoba berkomunikasi dengan alamat IP yang terkait dengan malware XOR DDoS.

Tingkat keparahan default: Tinggi

Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda mencoba berkomunikasi dengan alamat IP yang terkait dengan malware XOR DDoS. Instans EC2 ini mungkin disusupi. XOR DDoS adalah malware Trojan yang membajak sistem Linux. Untuk mendapatkan akses ke sistem, malware ini meluncurkan serangan brute force untuk memperoleh kata sandi ke layanan Secure Shell (SSH) di Linux. Setelah kredensial SSH diperoleh dan login berhasil dilakukan, malware ini menggunakan hak akses pengguna root untuk menjalankan skrip yang mengunduh dan menginstal XOR DDoS. Malware ini kemudian digunakan sebagai bagian dari botnet untuk meluncurkan serangan Penolakan Layanan Terdistribusi (DDoS) terhadap target lainnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

Behavior:IAMUser/InstanceLaunchUnusual

Pengguna meluncurkan jenis instans EC2 yang tidak biasa.

Tingkat keparahan default: Tinggi

Temuan ini memberi tahu Anda bahwa pengguna tertentu di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Pengguna ini tidak memiliki riwayat meluncurkan instans EC2 jenis ini sebelumnya. Kredensial masuk Anda mungkin disusupi.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.

CryptoCurrency:EC2/BitcoinTool.A

Instans EC2 berkomunikasi dengan kolam penambangan Bitcoin.

Tingkat keparahan default: Tinggi

Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda berkomunikasi dengan kumpulan penambangan Bitcoin. Di bidang penambangan mata uang kripto, kolam penambangan adalah kumpulan sumber daya dari para penambang yang berbagi daya pemrosesan mereka melalui jaringan untuk membagi hadiahnya sesuai dengan jumlah pekerjaan yang mereka kontribusikan dalam memecahkan sebuah blok. Kecuali jika Anda menggunakan instans EC2 ini untuk penambangan Bitcoin, instans EC2 Anda mungkin disusupi.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan.

UnauthorizedAccess:IAMUser/UnusualASNCaller

API dipanggil dari alamat IP dari jaringan yang tidak biasa.

Tingkat keparahan default: Tinggi

Temuan ini menginformasikan bahwa aktivitas tertentu dipanggil dari alamat IP dari jaringan yang tidak biasa. Jaringan ini tidak pernah diamati di seluruh riwayat penggunaan AWS dari pengguna

yang dimaksud. Kegiatan ini dapat mencakup login konsol, upaya untuk meluncurkan instans EC2, membuat pengguna IAM baru, mengubah hak istimewa AWS Anda, dll. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Lihat informasi yang lebih lengkap di Memperbaiki potensi terganggu AWS credentials.

GuardDuty menemukan jenis dengan sumber daya yang berpotensi terkena dampak

Halaman-halaman berikut dikategorikan berdasarkan jenis sumber daya yang berpotensi terkena dampak yang terkait dengan GuardDuty temuan:

- Tipe temuan EC2
- Tipe temuan IAM
- Jenis pencarian urutan serangan
- Jenis pencarian Aturan Deteksi Kustom
- Jenis temuan perlindungan S3
- Jenis penemuan Perlindungan EKS
- Jenis penemuan Runtime Monitoring
- Perlindungan Malware untuk jenis pencarian EC2
- Perlindungan Malware untuk tipe pencarian S3
- Perlindungan Malware untuk jenis pencarian Backup
- Jenis temuan Perlindungan RDS
- Jenis temuan Perlindungan Lambda
- Jenis penemuan Perlindungan AI

GuardDuty jenis temuan aktif

Tabel berikut menunjukkan semua jenis temuan aktif, dikelompokkan berdasarkan sumbernya: pertama jenis temuan dari deteksi ancaman dasar (diurutkan berdasarkan sumber data), kemudian

jenis pencarian urutan Deteksi Ancaman yang Diperpanjang serangan, dan kemudian jenis temuan dari setiap rencana perlindungan (dalam urutan abjad berdasarkan rencana). Dalam tabel berikut, beberapa temuan memiliki nilai kolom Finding severity yang ditandai dengan tanda bintang (*) atau tanda plus (+):

* Jenis temuan ini memiliki tingkat keparahan yang bervariasi. Temuan jenis tertentu mungkin memiliki tingkat keparahan yang berbeda tergantung pada konteks khusus untuk temuan tersebut. Untuk informasi selengkapnya tentang jenis temuan, lihat deskripsi detailnya.

+ Temuan EC2 yang menggunakan log aliran VPC sebagai sumber data tidak mendukung lalu lintas IPv6.

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Sedang
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Sedang
DefenseEvasion:IAMUser/BedrockLoggingDisabled	IAM	CloudTrail acara manajemen	Sedang
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Rendah
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Tinggi
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Tinggi
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Sedang

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
PenTest:IAMUser/KaliLinux	IAM	CloudTrail acara manajemen	Sedang
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail acara manajemen	Sedang
PenTest:IAMUser/PentooLinux	IAM	CloudTrail acara manajemen	Sedang
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Sedang
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail acara manajemen	Rendah *
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail acara manajemen	Tinggi *
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail acara manajemen	Rendah
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail acara manajemen	Tinggi
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail acara manajemen	Rendah
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail acara manajemen	Tinggi

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Sedang
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail acara manajemen	Sedang
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail acara manajemen	Sedang
Recon:IAMUser/TorIPCaller	IAM	CloudTrail acara manajemen	Sedang
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail acara manajemen	Rendah
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail acara manajemen	Rendah
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail acara manajemen	Sedang
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail acara manajemen	Sedang
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail acara manajemen	Sedang
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail acara manajemen	Sedang

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
CredentialAccess:IAMUser/CompromisedCredentials	IAM	CloudTrail peristiwa manajemen atau peristiwa CloudTrail data untuk S3	Tinggi
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail peristiwa manajemen atau peristiwa CloudTrail data untuk S3	Rendah
Policy:IAMUser/ShortTermRootCredentialUsage	IAM	CloudTrail peristiwa manajemen atau peristiwa CloudTrail data untuk S3	Rendah
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail peristiwa manajemen atau peristiwa CloudTrail data untuk S3	Tinggi
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS	IAM	CloudTrail peristiwa manajemen atau peristiwa CloudTrail data untuk S3	Tinggi
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	IAM	CloudTrail peristiwa manajemen atau peristiwa CloudTrail data untuk S3	Tinggi
Impact:EC2/MaliciousDomainRequest.Custom	Amazon EC2	Log DNS	Sedang

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	Log DNS	Tinggi
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	Log DNS	Tinggi
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	Log DNS	Sedang
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	Log DNS	Tinggi
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	Log DNS	Tinggi
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	Log DNS	Rendah
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	Log DNS	Sedang
Trojan:EC2/DGADomainRequest.B	Amazon EC2	Log DNS	Tinggi
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	Log DNS	Tinggi
Trojan:EC2/DNSDataExfiltration	Amazon EC2	Log DNS	Tinggi

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	Log DNS	Tinggi
Trojan:EC2/DropPoint!DNS	Amazon EC2	Log DNS	Sedang
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	Log DNS	Tinggi
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	Log DNS	Tinggi
Backdoor:EC2/C&CActivity.B	Amazon EC2	Log aliran VPC ±	Tinggi
Backdoor:EC2/DenialOfService.Dns	Amazon EC2	Log aliran VPC ±	Tinggi
Backdoor:EC2/DenialOfService.Tcp	Amazon EC2	Log aliran VPC ±	Tinggi
Backdoor:EC2/DenialOfService.Udp	Amazon EC2	Log aliran VPC ±	Tinggi
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	Amazon EC2	Log aliran VPC ±	Tinggi
Backdoor:EC2/DenialOfService.UnusualProtocol	Amazon EC2	Log aliran VPC ±	Tinggi
Backdoor:EC2/Spambot	Amazon EC2	Log aliran VPC ±	Sedang

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
Behavior:EC2/NetworkPortUnusual	Amazon EC2	Log aliran VPC [+]	Sedang
Behavior:EC2/TrafficVolumeUnusual	Amazon EC2	Log aliran VPC [+]	Sedang
CryptoCurrency:EC2/BitcoinTool.B	Amazon EC2	Log aliran VPC [+]	Tinggi
DefenseEvasion:EC2/UnusualDNSResolver	Amazon EC2	Log aliran VPC [+]	Sedang
DefenseEvasion:EC2/UnusualDoHActivity	Amazon EC2	Log aliran VPC [+]	Sedang
DefenseEvasion:EC2/UnusualDoTActivity	Amazon EC2	Log aliran VPC [+]	Sedang
Impact:EC2/PortSweep	Amazon EC2	Log aliran VPC [+]	Tinggi
Impact:EC2/WinRMBruteForce	Amazon EC2	Log aliran VPC [+]	Rendah [*]
Recon:EC2/PortProbeEMRUnprotectedPort	Amazon EC2	Log aliran VPC [+]	Tinggi
Recon:EC2/PortProbeUnprotectedPort	Amazon EC2	Log aliran VPC [+]	Rendah [*]
Recon:EC2/Portscan	Amazon EC2	Log aliran VPC [+]	Sedang
Trojan:EC2/BlackholeTraffic	Amazon EC2	Log aliran VPC [+]	Sedang

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
Trojan:EC2/DropPoint	Amazon EC2	Log aliran VPC [+]	Sedang
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Amazon EC2	Log aliran VPC [+]	Sedang
UnauthorizedAccess:EC2/RDPBruteForce	Amazon EC2	Log aliran VPC [+]	Rendah [*]
UnauthorizedAccess:EC2/SSHBruteForce	Amazon EC2	Log aliran VPC [+]	Rendah [*]
UnauthorizedAccess:EC2/TorClient	Amazon EC2	Log aliran VPC [+]	Tinggi
UnauthorizedAccess:EC2/TorRelay	Amazon EC2	Log aliran VPC [+]	Tinggi

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
AttackSequence:EKS/CompromisedCluster	Sumber daya yang terlibat dalam urutan serangan	• Kejadian log audit EKS • Pemantauan Runtime untuk Amazon EKS • Deteksi malware Amazon EKS untuk Amazon EC2 • AWS CloudTrail peristiwa data untuk S3 • AWS CloudTrail acara manajemen • Log Alur VPC • Log kueri DNS Route53 Resolver	Kritis
AttackSequence:IAM/CompromisedCredentials	Sumber daya yang terlibat dalam urutan serangan	CloudTrail acara manajemen	Kritis
AttackSequence:S3/CompromisedData	Sumber daya yang terlibat dalam urutan serangan	CloudTrail acara manajemen dan peristiwa CloudTrail data untuk S3	Kritis

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
AttackSequence:ECS/CompromisedCluster	Sumber daya yang terlibat dalam urutan serangan	• AWS Deteksi Runtime Amazon ECS (Fargate) • AWS Deteksi Runtime Amazon ECS (Instans Amazon EC2) • AWS Deteksi malware	Kritis
AttackSequence:EC2/CompromisedInstanceGroup	Sumber daya yang terlibat dalam urutan serangan	• AWS Deteksi Runtime Amazon EC2 • AWS Deteksi malware • Log Alur VPC • Log kueri DNS Route53 Resolver	Kritis
Impact:IAMUser/AnomalousModelInvocation	IAM	Perlindungan AI	Rendah
Impact:IAMUser/CostHarvesting	IAM	Perlindungan AI	Rendah
Impact:IAMUser/PromptInjection.Direct	IAM	Perlindungan AI	Rendah
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	Log audit EKS	Sedang

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	Log audit EKS	Tinggi
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log audit EKS	Tinggi
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log audit EKS	Tinggi
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	Log audit EKS	Tinggi
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	Log audit EKS	Tinggi
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log audit EKS	Tinggi
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log audit EKS	Tinggi
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	Log audit EKS	Tinggi
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	Log audit EKS	Rendah

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	Log audit EKS	Sedang
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log audit EKS	Sedang
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log audit EKS	Sedang
Discovery:Kubernetes/TorIPCaller	Kubernetes	Log audit EKS	Sedang
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	Log audit EKS	Sedang
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	Log audit EKS	Sedang
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	Log audit EKS	Rendah
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	Log audit EKS	Tinggi
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log audit EKS	Tinggi
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log audit EKS	Tinggi

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
Impact:Kubernetes/TorIPCaller	Kubernetes	Log audit EKS	Tinggi
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	Log audit EKS	Sedang
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log audit EKS	Sedang
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log audit EKS	Tinggi
Persistence:Kubernetes/TorIPCaller	Kubernetes	Log audit EKS	Sedang
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	Log audit EKS	Tinggi
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	Log audit EKS	Tinggi
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	Log audit EKS	Sedang
Policy:Kubernetes/ExposedDashboard	Kubernetes	Log audit EKS	Sedang
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	Log audit EKS	Sedang *

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	Log audit EKS	Rendah
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	Log audit EKS	Tinggi
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	Log audit EKS	Tinggi
Backdoor:Lambda/C&CActivity.B	Lambda	Pemantauan Aktivitas Jaringan Lambda	Tinggi
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Pemantauan Aktivitas Jaringan Lambda	Tinggi
Trojan:Lambda/BlackholeTraffic	Lambda	Pemantauan Aktivitas Jaringan Lambda	Sedang
Trojan:Lambda/DropPoint	Lambda	Pemantauan Aktivitas Jaringan Lambda	Sedang
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Pemantauan Aktivitas Jaringan Lambda	Sedang
UnauthorizedAccess:Lambda/TorClient	Lambda	Pemantauan Aktivitas Jaringan Lambda	Tinggi

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
UnauthorizedAccess:Lambda/TorRelay	Lambda	Pemantauan Aktivitas Jaringan Lambda	Tinggi
Execution:Container/MaliciousFile	Kontainer	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:Container/SuspiciousFile	Kontainer	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:EC2/MaliciousFile	Amazon EC2	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:EC2/SuspiciousFile	Amazon EC2	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:ECS/MaliciousFile	ECS	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:ECS/SuspiciousFile	ECS	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:Kubernetes/MaliciousFile	Kubernetes	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:Kubernetes/SuspiciousFile	Kubernetes	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
Execution:EC2/MaliciousFile!Snapshot	Amazon EBS	Perlindungan Malware untuk Backup	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:EC2/MaliciousFile!AMI	Amazon EC2	Perlindungan Malware untuk Backup	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:EC2/MaliciousFile!RecoveryPoint	AWS Backup	Perlindungan Malware untuk Backup	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:S3/MaliciousFile!RecoveryPoint	AWS Backup	Perlindungan Malware untuk Backup	Bervariasi tergantung pada ancaman yang terdeteksi
Object:S3/MaliciousFile	S3Object	Perlindungan Malware untuk S3	Tinggi
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Rendah
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Tinggi
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Variabel *

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Sedang
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Tinggi
CredentialAccess:RDS/TorIPCaller.FailedLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Sedang
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Tinggi
Discovery:RDS/MaliciousIPCaller	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Sedang
Discovery:RDS/TorIPCaller	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Sedang
Exfiltration:RDS/AnomalousBehavior	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas RDS DB	Rendah *

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
Exfiltration:RDS/MaliciousIPCaller	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas RDS DB	Tinggi
Exfiltration:RDS/TorIPCaller	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas RDS DB	Tinggi
Impact:RDS/AnomalousBehavior.Delete	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas RDS DB	Rendah *
Impact:RDS/AnomalousBehavior.Drop	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas RDS DB	Sedang *
Impact:RDS/MaliciousIPCaller	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas RDS DB	Tinggi
Impact:RDS/TorIPCaller	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas RDS DB	Tinggi
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail peristiwa data untuk S3	Rendah
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail peristiwa data untuk S3	Sedang
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail peristiwa data untuk S3	Sedang
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
PenTest:S3/KaliLinux	Amazon S3	CloudTrail peristiwa data untuk S3	Sedang
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail peristiwa data untuk S3	Sedang
PenTest:S3/PentooLinux	Amazon S3	CloudTrail peristiwa data untuk S3	Sedang
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Backdoor:Runtime/C&CActivity.B	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Tinggi
Backdoor:Runtime/C&CActivity.B!DNS	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Tinggi
CryptoCurrency:Runtime/BitcoinTool.B	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
DefenseEvasion:Runtime/FilelessExecution	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
DefenseEvasion:Runtime/KernelModuleLoaded	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
DefenseEvasion:Runtime/SensitiveFileModified	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
DefenseEvasion:Runtime/ProcessInjection.Proc	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
DefenseEvasion:Runtime/PtraceAntiDebugging	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Rendah
DefenseEvasion:Runtime/SuspiciousCommand	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Discovery:Runtime/SuspiciousCommand	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Rendah
Execution:Runtime/MaliciousFileExecuted	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Execution:Runtime/MaliciousFileExecuted.Custom	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Execution:Runtime/NewBinaryExecuted	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Execution:Runtime/NewLibraryLoaded	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
Execution:Runtime/SuspiciousCommand	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Variabel
Execution:Runtime/SuspiciousShellCreated	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Rendah
Execution:Runtime/SuspiciousTool	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Variabel
Execution:Runtime/ReverseShell	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Impact:Runtime/AbusedDomainRequest.Reputation	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Impact:Runtime/BitcoinDomainRequest.Reputation	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Impact:Runtime/CryptoMinerExecuted	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Impact:Runtime/MaliciousDomainRequest.Reputation	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Impact:Runtime/SuspiciousDomainRequest.Reputation	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Rendah

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
Persistence:Runtime/SuspiciousCommand	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Persistence:Runtime/SensitiveFileModified	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
PrivilegeEscalation:Runtime/DockerSocketAccessed	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
PrivilegeEscalation:Runtime/ElevationToRoot	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
PrivilegeEscalation:Runtime/RuncContainerEscape	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
PrivilegeEscalation:Runtime/SuspiciousCommand	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
PrivilegeEscalation:Runtime/SensitiveFileModified	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
PrivilegeEscalation:Runtime/UserfaultfdUsage	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Trojan:Runtime/BlackholeTraffic	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Trojan:Runtime/BlackholeTraffic! DNS	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Trojan:Runtime/DropPoint	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Trojan:Runtime/DGADomainRequest.C! DNS	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Trojan:Runtime/DriveBySourceTraffic! DNS	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Trojan:Runtime/DropPoint! DNS	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Trojan:Runtime/PhishingDomainRequest! DNS	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
UnauthorizedAccess:Runtime/MetadataDNSRebind	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi

Tipe temuan	Tipe sumber daya	Data dasar source/Feature	Menemukan tingkat keparahan
UnauthorizedAccess:Runtime/TorClient	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
UnauthorizedAccess:Runtime/TorRelay	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi

Memahami dan menghasilkan GuardDuty temuan Amazon

Tem GuardDuty uan mewakili masalah keamanan potensial yang terdeteksi di dalam Akun AWS, beban kerja, dan data. GuardDuty menghasilkan temuan setiap kali mendeteksi aktivitas tak terduga dan berpotensi berbahaya di AWS lingkungan Anda.

Anda dapat melihat dan mengelola GuardDuty temuan Anda di halaman Temuan di GuardDuty konsol, atau dengan menggunakan operasi API or. AWS CLI Untuk informasi tentang bagaimana Anda dapat mengelola GuardDuty temuan, lihatMengelola GuardDuty temuan Amazon.

Topik:

GuardDuty menemukan format

Memahami format jenis GuardDuty pencarian dan berbagai tujuan ancaman yang dil GuardDuty acak.

Sampel temuan

Hasilkan temuan sampel di GuardDuty konsol, atau dengan menggunakan GuardDuty API atau AWS CLI perintah. Temuan sampel yang dihasilkan mencakup detail fiktif untuk membantu Anda memahami detail temuan yang terkait dengan setiap GuardDuty temuan. Temuan ini ditandai dengan awalan [SAMPLE].

GuardDuty Temuan uji di akun khusus

Anda dapat menguji GuardDuty temuan spesifik di lingkungan Anda. Jalan `guardduty-tester` kan skrip dalam non-produksi Akun AWS khusus. GuardDuty Untuk mendeteksi dan mensimulasikan temuan, itu akan menyebarkan sumber daya tertentu di lingkungan Anda. Pengalaman ini berbeda dengan menghasilkan temuan sampel.

Melihat temuan yang dihasilkan di GuardDuty konsol

Pelajari cara meninjau temuan yang dihasilkan di GuardDuty konsol.

Tingkat keparahan GuardDuty temuan

Setiap GuardDuty temuan memiliki tingkat keparahan terkait yang mencerminkan potensi risiko di AWS lingkungan Anda. Bagian ini menjelaskan apa yang ditandai oleh setiap tingkat keparahan.

Detail temuan

Pelajari detail yang terkait dengan GuardDuty temuan yang dihasilkan di akun Anda. Topik ini mencakup detail yang terkait dengan deteksi ancaman dasar, Deteksi Ancaman yang Diperpanjang, dan rencana perlindungan khusus di GuardDuty.

GuardDuty menemukan agregasi

Pelajari cara GuardDuty menangani beberapa kejadian dari jenis temuan yang sama. Dengan menggabungkan jenis temuan yang sama yang terdeteksi GuardDuty, perbarui jenis temuan asli dengan detail terbaru.

GuardDuty menemukan jenis

Bagian ini mencantumkan GuardDuty jenis pencarian berdasarkan Sumber data dasar atau Fitur yang dipetakan GuardDuty yang terkait. Untuk mempelajari tentang setiap jenis temuan, pilih temuan itu untuk detail lebih lanjut, seperti deskripsi dan langkah-langkah potensial untuk memperbaiki temuan.

GuardDuty menemukan format

Ketika GuardDuty mendeteksi perilaku mencurigakan atau tidak terduga di AWS lingkungan Anda, itu menghasilkan temuan. Temuan adalah pemberitahuan yang berisi rincian tentang potensi masalah keamanan yang GuardDuty ditemukan. Melihat temuan yang dihasilkan di GuardDuty konsolTermasuk informasi tentang apa yang terjadi, AWS sumber daya mana yang terlibat dalam aktivitas mencurigakan, kapan kegiatan ini berlangsung, dan informasi terkait yang dapat membantu Anda memahami akar penyebabnya.

Salah satu bagian informasi yang paling berguna dalam detail temuan adalah jenis temuan. Tujuan dari jenis temuan adalah untuk memberikan deskripsi ringkas namun dapat dibaca tentang potensi masalah keamanan. Misalnya, tipe GuardDuty Recon:EC2/PortProbeUnprotectedPorttemuan dengan cepat memberi tahu Anda bahwa di suatu tempat di AWS lingkungan Anda, instans EC2 memiliki port yang tidak dilindungi yang sedang diselidiki oleh penyerang potensial.

GuardDuty menggunakan format berikut untuk menamai berbagai jenis temuan yang dihasilkannya:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism! Artifak

Setiap bagian dari format ini mewakili aspek dari jenis temuan. Aspek-aspek ini memiliki penjelasan sebagai berikut:

- ThreatPurpose- menggambarkan tujuan utama dari ancaman, jenis serangan atau tahap serangan potensial. Lihat bagian berikut untuk daftar lengkap tujuan GuardDuty ancaman.
- ResourceTypeAffected- menjelaskan jenis AWS sumber daya mana yang diidentifikasi dalam temuan ini sebagai target potensial musuh. Saat ini, GuardDuty dapat menghasilkan temuan untuk jenis sumber daya yang tercantum dalamGuardDuty jenis temuan aktif.
- ThreatFamilyName- menggambarkan ancaman keseluruhan atau potensi aktivitas jahat GuardDuty yang mendeteksi. Misalnya, nilai NetworkPortUnusualmenunjukkan bahwa instans EC2 yang diidentifikasi dalam GuardDuty temuan tidak memiliki riwayat komunikasi sebelumnya pada port jarak jauh tertentu yang juga diidentifikasi dalam temuan.
- DetectionMechanism- menjelaskan metode di mana GuardDuty mendeteksi temuan. Ini dapat digunakan untuk menunjukkan variasi pada jenis temuan umum atau temuan yang GuardDuty menggunakan mekanisme khusus untuk mendeteksi. Misalnya, Backdoor:EC2/DenialOfService.Tcpmenunjukkan penolakan layanan (DoS) terdeteksi melalui TCP. Varian UDP adalah Backdoor:EC2/DenialOfService.Udp.

  Nilai .Custom menunjukkan bahwa GuardDuty mendeteksi temuan berdasarkan daftar ancaman kustom Anda. Untuk informasi selengkapnya, lihat Daftar entitas dan daftar alamat IP.

  Nilai .Reputation menunjukkan bahwa GuardDuty mendeteksi temuan menggunakan model skor reputasi domain. Untuk informasi selengkapnya, lihat Cara AWS melacak ancaman keamanan terbesar cloud dan membantu mematikannya.
- Artifact - menjelaskan sumber daya tertentu yang dimiliki oleh alat yang digunakan dalam aktivitas berbahaya. Misalnya, DNS dalam tipe temuan CryptoCurrency:EC2/BitcoinTool.B!DNS menunjukkan bahwa instans Amazon EC2 berkomunikasi dengan domain yang dikenal. Bitcoin-related

> **Note**
>
> Artifak bersifat opsional dan mungkin tidak tersedia untuk semua jenis GuardDuty temuan.

Tujuan Ancaman

Dalam tujuan GuardDuty ancaman menggambarkan tujuan utama dari ancaman, jenis serangan, atau tahap serangan potensial. Misalnya, beberapa tujuan ancaman, seperti Backdoor, menunjukkan jenis serangan. Namun, beberapa tujuan ancaman, seperti Impact sejajar dengan taktik MITRE

ATT&CK. Taktik MITRE ATT&CK menunjukkan fase yang berbeda dalam siklus serangan musuh. Dalam rilis saat ini GuardDuty, ThreatPurpose dapat memiliki nilai-nilai berikut:

Pintu Belakang

Nilai ini menunjukkan bahwa musuh telah mengkompromikan AWS sumber daya dan mengubah sumber daya sehingga mampu menghubungi server home command and control (C&C) untuk menerima instruksi lebih lanjut untuk aktivitas berbahaya.

Perilaku

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang berbeda dari garis dasar yang ditetapkan untuk AWS sumber daya yang terlibat.

CredentialAccess

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi pola aktivitas yang mungkin digunakan musuh untuk mencuri kredensil, seperti kata sandi, nama pengguna, dan kunci akses, dari lingkungan Anda. Tujuan ancaman ini didasarkan pada taktik MITRE ATT&CK.

Cryptocurrency

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi bahwa AWS sumber daya di lingkungan Anda adalah perangkat lunak hosting yang terkait dengan cryptocurrency (misalnya, Bitcoin).

DefenseEvasion

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang mungkin digunakan musuh untuk menghindari deteksi saat menyusup ke lingkungan Anda. Tujuan ancaman ini didasarkan pada taktik MITRE ATT&CK

Penemuan

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang dapat digunakan musuh untuk memperluas pengetahuan mereka tentang sistem dan jaringan internal Anda. Tujuan ancaman ini didasarkan pada taktik MITRE ATT&CK.

Eksekusi

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi bahwa musuh dapat mencoba menjalankan atau telah menjalankan kode berbahaya untuk menjelajahi AWS lingkungan, atau mencuri data. Tujuan ancaman ini didasarkan pada taktik MITRE ATT&CK.

Ekfiltrasi

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang mungkin digunakan musuh saat mencoba mencuri data dari lingkungan Anda. Tujuan ancaman ini didasarkan pada taktik MITRE ATT&CK.

Dampak

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang menunjukkan bahwa musuh sedang mencoba memanipulasi, mengganggu, atau menghancurkan sistem dan data Anda. Tujuan ancaman ini didasarkan pada taktik MITRE ATT&CK.

InitialAccess

Nilai ini umumnya dikaitkan dengan tahap akses awal serangan ketika musuh mencoba untuk membangun akses ke lingkungan Anda. Tujuan ancaman ini didasarkan pada taktik MITRE ATT&CK.

Pentest

Terkadang pemilik AWS sumber daya atau perwakilan resmi mereka sengaja menjalankan tes terhadap AWS aplikasi untuk menemukan kerentanan, seperti grup keamanan terbuka atau kunci akses yang terlalu permisif. Uji penetrasi ini dilakukan dalam upaya untuk mengidentifikasi dan mengunci sumber daya yang rentan sebelum ditemukan oleh musuh. Namun, beberapa alat yang digunakan oleh penguji penetrasi resmi tersedia secara bebas dan oleh karena itu dapat digunakan oleh pengguna yang tidak sah atau musuh untuk menjalankan uji probing. Meskipun tidak GuardDuty dapat mengidentifikasi tujuan sebenarnya di balik aktivitas tersebut, nilai Pentest menunjukkan bahwa GuardDuty mendeteksi aktivitas tersebut, bahwa itu mirip dengan aktivitas yang dihasilkan oleh alat pengujian pena yang diketahui, dan bahwa itu dapat menunjukkan penyelidikan berbahaya pada jaringan Anda.

Kegigihan

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang dapat digunakan musuh untuk mencoba dan mempertahankan akses ke sistem Anda bahkan jika rute akses awal mereka terputus. Misalnya, ini dapat termasuk membuat pengguna IAM baru setelah mendapatkan akses menggunakan kredensial pengguna yang ada. Ketika kredensial pengguna yang ada dihapus, musuh akan mempertahankan akses pada pengguna baru yang tidak terdeteksi sebagai bagian dari peristiwa asli. Tujuan ancaman ini didasarkan pada taktik MITRE ATT&CK.

Kebijakan

Nilai ini menunjukkan bahwa Anda Akun AWS menunjukkan perilaku yang bertentangan dengan praktik terbaik keamanan yang direkomendasikan. Misalnya, modifikasi kebijakan izin yang tidak disengaja yang terkait dengan AWS sumber daya atau lingkungan Anda, dan penggunaan akun istimewa yang seharusnya memiliki sedikit atau tidak ada penggunaan.

PrivilegeEscalation

Nilai ini menginformasikan bahwa prinsipal yang terlibat dalam lingkungan AWS Anda menunjukkan perilaku yang mungkin digunakan musuh untuk mendapatkan izin dengan tingkat yang lebih tinggi ke jaringan Anda. Tujuan ancaman ini didasarkan pada taktik MITRE ATT&CK.

Pengintaian

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang mungkin digunakan musuh saat melakukan pengintaian terhadap lingkungan Anda untuk menentukan bagaimana mereka dapat memperluas akses mereka atau memanfaatkan sumber daya Anda. Misalnya, aktivitas ini dapat mencakup pelingkupan kerentanan di AWS lingkungan Anda dengan memeriksa port, membuat panggilan API, mencantumkan pengguna, dan mencantumkan tabel database.

Siluman

Nilai ini menunjukkan bahwa musuh secara aktif mencoba menyembunyikan tindakan mereka. Misalnya, mereka mungkin menggunakan server proksi anonim, sehingga sangat sulit untuk mengukur sifat sebenarnya dari aktivitas tersebut.

Trojan

Nilai ini menunjukkan bahwa serangan menggunakan program Trojan yang diam-diam melakukan aktivitas berbahaya. Terkadang perangkat lunak ini mengambil tampilan program yang sah. Terkadang pengguna secara tidak sengaja menjalankan perangkat lunak ini. Lain kali perangkat lunak ini mungkin berjalan secara otomatis dengan memanfaatkan kerentanan.

UnauthorizedAccess

Nilai ini menunjukkan bahwa GuardDuty mendeteksi aktivitas mencurigakan atau pola aktivitas yang mencurigakan oleh individu yang tidak berwenang.

GuardDuty mesin pemindai deteksi malware

Amazon GuardDuty memiliki mesin pemindaian yang dibangun dan dikelola secara internal dan vendor pihak ketiga. Keduanya menggunakan indikator kompromi (IoCs) yang bersumber dari berbagai feed internal yang memiliki visibilitas di berbagai jenis malware yang mungkin ditargetkan. AWS GuardDuty juga memiliki definisi deteksi yang didasarkan pada aturan YARA yang ditambahkan oleh teknisi keamanan kami, dan deteksi berdasarkan model heuristik dan pembelajaran mesin (ML). Saat memindai objek Amazon S3, Perlindungan GuardDuty Malware menghasilkan hasil yang konsisten saat memindai objek yang sama beberapa kali dengan definisi dan mesin pemindaian yang sama. Signature-based deteksi tidak hanya mencakup pencocokan byte tetapi juga potongan kode yang berpotensi kompleks, dan pemindai dapat mengurai konten dan membuat keputusan.

Mesin pemindai malware tidak melakukan analisis perilaku langsung, di mana peledakan malware memantau sampel saat dijalankan dalam sistem nyata. GuardDuty Solusinya terutama deteksi berbasis file. Untuk mendeteksi malware tanpa file, GuardDuty berikan solusi berbasis agen, seperti untuk Pemantauan Runtime Amazon EKS, Amazon EC2, dan Amazon ECS (termasuk). AWS Fargate

Tanpa batasan pada format file yang GuardDuty memindai malware, mesin pemindai yang digunakannya dapat mendeteksi berbagai jenis malware, seperti cryptominers, ransomware, dan webshell. Mesin GuardDuty pemindaian yang dikelola sepenuhnya terus memperbarui daftar tanda tangan malware setiap 15 menit.

Mesin pemindai adalah bagian dari sistem intelijen GuardDuty ancaman yang menggunakan komponen peledakan malware internal. Ini menghasilkan intelijen ancaman baru dengan mengumpulkan malware dan sampel jinak secara independen dari berbagai sumber. File hash tipe IoC dari sistem intelijen ancaman selanjutnya dimasukkan ke mesin pemindaian malware untuk mendeteksi malware berdasarkan hash file buruk yang diketahui.

Menghasilkan temuan sampel di GuardDuty

Amazon GuardDuty membantu Anda menghasilkan temuan sampel untuk memvisualisasikan dan memahami berbagai jenis temuan yang dapat dihasilkannya. Saat Anda menghasilkan temuan sampel, GuardDuty isi daftar temuan Anda saat ini dengan satu sampel untuk setiap jenis temuan yang didukung, termasuk jenis pencarian urutan serangan.

Sampel yang dibuat adalah perkiraan yang diisi dengan nilai placeholder. Sampel ini mungkin terlihat berbeda dari temuan nyata untuk lingkungan Anda, tetapi Anda dapat menggunakannya untuk

menguji berbagai konfigurasi GuardDuty, seperti EventBridge acara atau filter Anda. Untuk daftar nilai yang tersedia untuk menemukan jenis, lihat GuardDuty menemukan jenis tabel.

Menghasilkan temuan sampel melalui GuardDuty konsol atau API

Pilih metode akses pilihan Anda untuk menghasilkan temuan sampel.

> **Note**
>
> Kon GuardDuty sol membantu Anda menghasilkan satu dari setiap jenis temuan. Untuk menghasilkan satu atau lebih jenis temuan spesifik, lakukan API/CLI langkah-langkah terkait.

Console

Gunakan prosedur berikut untuk membuat sampel temuan. Proses ini menghasilkan satu temuan sampel untuk setiap jenis GuardDuty temuan.

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di halaman Pengaturan, di bawah Sampel temuan, pilih Buat sampel temuan.
4. Di panel navigasi, pilih Temuan. Sampel temuan ditampilkan di halaman Temuan saat ini dengan prefiks [SAMPLE].

API/CLI

Anda dapat menghasilkan satu sampel temuan yang cocok dengan salah satu jenis tem GuardDuty uan melalui CreateSampleFindings API, nilai yang tersedia untuk menemukan jenis tercantum dalam GuardDuty menemukan jenis tabel.

Ini berguna untuk pengujian aturan Acara CloudWatch atau otomatisasi berdasarkan temuan. Contoh berikut menunjukkan cara menghasilkan temuan sampel tunggal dari `Backdoor:EC2/DenialOfService.Tcp` jenis menggunakan AWS CLI.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

Judul temuan sampel yang dihasilkan melalui metode ini selalu dimulai dengan [SAMPLE] di konsol. Temuan sampel memiliki nilai `"sample": true` di bagian AdditionalInfo dari rincian JSON penemuan.

Untuk memahami detail temuan, seperti menemukan tingkat keparahan dan sumber daya yang berpotensi dikompromikan, terkait dengan temuan yang dihasilkan, lihat Tingkat keparahan GuardDuty temuan danDetail temuan.

Untuk menghasilkan beberapa temuan umum berdasarkan aktivitas simulasi dalam lingkungan yang didedikasikan dan terisolasi Akun AWS di lingkungan Anda, lihatGuardDuty Temuan uji di akun khusus.

GuardDuty Temuan uji di akun khusus

Gunakan dokumen ini untuk menjalankan skrip penguji yang menghasilkan GuardDuty temuan terhadap sumber daya pengujian yang akan digunakan di file Anda. Akun AWS Anda dapat melakukan langkah-langkah ini ketika Anda ingin memahami dan mempelajari tentang jenis GuardDuty temuan tertentu dan bagaimana rincian temuan mencari sumber daya aktual di akun Anda. Pengalaman ini berbeda dengan menghasilkanSampel temuan. Untuk informasi lebih lanjut tentang pengalaman pengujian GuardDuty temuan, lihatPertimbangan-pertimbangan.

Daftar Isi

- Pertimbangan-pertimbangan
- GuardDuty temuan skrip tester dapat menghasilkan
- Langkah 1 - Prasyarat
- Langkah 2 - Menyebarkan sumber daya AWS
- Langkah 3 - Jalankan skrip penguji
- Langkah 4 - Bersihkan sumber daya AWS tes
- Memecahkan masalah umum

Pertimbangan-pertimbangan

Sebelum Anda melanjutkan, pertimbangkan pertimbangan berikut:

- GuardDuty merekomendasikan untuk menggunakan tester dalam non-produksi khusus. Akun AWS Pendekatan ini akan memastikan bahwa Anda dapat mengidentifikasi GuardDuty temuan yang dihasilkan oleh penguji dengan benar. Selain itu, GuardDuty penguji menyebarkan berbagai sumber daya yang mungkin memerlukan izin IAM di luar apa yang diizinkan di akun lain. Menggunakan akun khusus memastikan bahwa izin dapat dicakup dengan benar dengan batas akun yang jelas.
- Skrip tester menghasilkan lebih dari 100 GuardDuty temuan dengan kombinasi AWS sumber daya yang berbeda. Saat ini, ini tidak termasuk semua. GuardDuty menemukan jenis Untuk daftar jenis pencarian yang dapat Anda hasilkan dengan skrip penguji ini, lihatGuardDuty temuan skrip tester dapat menghasilkan.

  > **Catatan**
  >
  > Untuk memvisualisasikan jenis pencarian urutan Attack, skrip tester hanya AttackSequence:EKS/CompromisedCluster menghasilkan dan. AttackSequence:S3/CompromisedData Untuk memvisualisasikan dan memahamiAttackSequence:IAM/CompromisedCredentials, Anda dapat menghasilkan Sampel temuan di akun Anda.

- Agar GuardDuty penguji berfungsi seperti yang diharapkan, GuardDuty perlu diaktifkan di akun tempat sumber daya penguji digunakan. Bergantung pada pengujian yang akan dijalankan, penguji mengevaluasi apakah rencana GuardDuty perlindungan yang sesuai diaktifkan atau tidak. Untuk setiap rencana perlindungan yang tidak diaktifkan, GuardDuty akan meminta izin untuk mengaktifkan rencana perlindungan yang diperlukan cukup lama GuardDuty untuk melakukan tes yang akan menghasilkan temuan. Nanti, GuardDuty akan menonaktifkan rencana perlindungan setelah pengujian selesai.

  Mengaktifkan GuardDuty untuk pertama kalinya

  Ketika GuardDuty diaktifkan di akun khusus Anda untuk pertama kalinya di Wilayah tertentu, akun Anda akan secara otomatis terdaftar dalam uji coba gratis 30 hari.

  GuardDuty menawarkan paket perlindungan opsional. Pada saat memungkinkan GuardDuty, paket perlindungan tertentu juga diaktifkan dan termasuk dalam uji coba gratis GuardDuty 30 hari. Untuk informasi selengkapnya, lihat Menggunakan uji GuardDuty coba gratis 30 hari.

GuardDuty sudah diaktifkan di akun Anda sebelum menjalankan skrip penguji

Ketika sudah GuardDuty diaktifkan, maka berdasarkan parameter, skrip tester akan memeriksa status konfigurasi rencana perlindungan tertentu dan pengaturan tingkat akun lainnya yang diperlukan untuk menghasilkan temuan.

Dengan menjalankan skrip penguji ini, paket perlindungan tertentu mungkin diaktifkan untuk pertama kalinya di akun khusus Anda di Wilayah. Ini akan memulai uji coba gratis 30 hari untuk rencana perlindungan itu. Untuk informasi tentang uji coba gratis yang terkait dengan setiap paket perlindungan, lihatMenggunakan uji GuardDuty coba gratis 30 hari.

- Selama infrastruktur GuardDuty penguji diterapkan, Anda kadang-kadang dapat menerima UnauthorizedAccess:EC2/TorClient temuan dari instans. PenTest

GuardDuty temuan skrip tester dapat menghasilkan

Saat ini, skrip penguji menghasilkan jenis temuan berikut yang terkait dengan log audit Amazon EC2, Amazon EKS, Amazon S3, IAM, dan EKS:

- AttackSequence:EKS/CompromisedCluster
- AttackSequence:S3/CompromisedData
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Udp
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint!DNS

- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- PenTest:IAMUser/KaliLinux
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- PenTest:S3/KaliLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled

- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller
- Backdoor:Runtime/C&CActivity.B! DNS
- CryptoCurrency:Runtime/BitcoinTool.B! DNS
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- Trojan:Runtime/BlackholeTraffic! DNS
- Trojan:Runtime/DGADomainRequest.C! DNS
- Trojan:Runtime/DriveBySourceTraffic! DNS
- Trojan:Runtime/DropPoint! DNS
- Trojan:Runtime/PhishingDomainRequest! DNS

Langkah 1 - Prasyarat

Untuk mempersiapkan lingkungan pengujian Anda, Anda memerlukan item berikut:

- Git — Instal alat baris perintah git berdasarkan sistem operasi yang Anda gunakan.

  Ini diperlukan untuk mengkloning `amazon-guardduty-tester`repositori.
- AWS Command Line Interface— Alat open source yang memungkinkan Anda berinteraksi Layanan AWS dengan menggunakan perintah di shell baris perintah Anda. Untuk informasi selengkapnya, lihat Memulai AWS CLI di Panduan AWS Command Line Interface Pengguna.
- AWS Systems Manager— Untuk memulai sesi Session Manager dengan node terkelola Anda dengan menggunakan AWS CLI Anda harus menginstal plugin Session Manager di mesin lokal Anda. Untuk informasi selengkapnya, lihat Plugin Install Session Manager AWS CLI di Panduan AWS Systems Manager Pengguna.

- Node Package Manager (NPM) - Instal NPM untuk menginstal semua dependensi.
- Docker — Anda harus menginstal Docker. Untuk petunjuk penginstalan, lihat situs web Docker.

  Untuk memverifikasi bahwa Docker telah diinstal, jalankan perintah berikut dan konfirmasikan ada output yang mirip dengan output berikut:

```
$ docker --version
Docker version 19.03.1
```

- Berlangganan gambar Kali Linux di AWS Marketplace.

Langkah 2 - Menyebarkan sumber daya AWS

Bagian ini menyediakan daftar konsep kunci dan langkah-langkah untuk menyebarkan AWS sumber daya tertentu di akun khusus Anda.

Konsep

Daftar berikut menyediakan konsep kunci yang terkait dengan perintah yang membantu Anda menyebarkan sumber daya:

- AWS Cloud Development Kit (AWS CDK)CDK adalah kerangka pengembangan perangkat lunak open-source untuk mendefinisikan infrastruktur cloud dalam kode dan menyediakannya. CloudFormation CDK mendukung beberapa bahasa pemrograman untuk mendefinisikan komponen cloud yang dapat digunakan kembali yang dikenal sebagai konstruksi. Anda dapat menyusun ini bersama-sama ke tumpukan dan aplikasi. Kemudian, Anda dapat menerapkan aplikasi CDK Anda CloudFormation untuk menyediakan atau memperbarui sumber daya Anda. Untuk informasi lebih lanjut, lihat Apa itu AWS CDK? di Panduan AWS Cloud Development Kit (AWS CDK) Pengembang.
- Bootstrapping — Ini adalah proses mempersiapkan AWS lingkungan Anda untuk digunakan dengan. AWS CDK Sebelum Anda menyebarkan tumpukan CDK ke lingkungan, AWS lingkungan harus di-bootstrap terlebih dahulu. Proses penyediaan AWS sumber daya tertentu di lingkungan Anda yang digunakan oleh AWS CDK adalah bagian dari langkah-langkah yang akan Anda lakukan di bagian berikutnya -. Langkah-langkah untuk menyebarkan sumber daya AWS

  Untuk informasi selengkapnya tentang cara kerja bootstrap, lihat Bootstrapping di Panduan Pengembang.AWS Cloud Development Kit (AWS CDK)

Langkah-langkah untuk menyebarkan sumber daya AWS

Lakukan langkah-langkah berikut untuk mulai menerapkan sumber daya:

1. Siapkan akun AWS CLI default dan Wilayah kecuali variabel Wilayah akun khusus diatur secara manual dalam `bin/cdk-gd-tester.ts` file. Untuk informasi selengkapnya, lihat Lingkungan di Panduan AWS Cloud Development Kit (AWS CDK) Pengembang.
2. Jalankan perintah berikut untuk menyebarkan sumber daya:

```
git clone https://github.com/awslabs/amazon-guardduty-tester && cd amazon-guardduty-
tester
npm install
cdk bootstrap
cdk deploy
```

   Perintah terakhir (`cdk deploy`) membuat CloudFormation tumpukan atas nama Anda. Nama tumpukan ini adalah GuardDutyTesterStack.

   Sebagai bagian dari skrip ini, GuardDuty buat sumber daya baru untuk menghasilkan GuardDuty temuan di akun Anda. Ini juga menambahkan pasangan kunci tag berikut: nilai ke instans Amazon EC2:

   `CreatedBy:GuardDuty Test Script`

   Instans Amazon EC2 juga menyertakan instans EC2 yang menampung node EKS dan kluster ECS.

   > **Tipe instans**
   >
   > GuardDuty dirancang untuk menggunakan jenis instans hemat biaya yang memberikan kinerja minimum yang diperlukan untuk berhasil melaksanakan pengujian. Karena persyaratan vCPU, grup node Amazon EKS memerlukan`t3.medium`, dan karena peningkatan kapasitas jaringan yang diperlukan untuk DenialOfService menemukan pengujian, node driver memerlukan. `m6i.large` Untuk semua tes lainnya, GuardDuty gunakan tipe `t3.micro` instance. Untuk informasi selengkapnya tentang jenis instans, lihat Ukuran yang tersedia di Panduan Jenis Instans Amazon EC2.

Langkah 3 - Jalankan skrip penguji

Ini adalah proses dua langkah di mana Anda pertama-tama perlu memulai sesi dengan driver uji dan kemudian, jalankan skrip untuk menghasilkan GuardDuty temuan dengan kombinasi sumber daya tertentu.

Bagian A - Mulai sesi dengan driver tes

1. Setelah resource Anda di-deploy, simpan kode Region ke variabel di sesi terminal Anda saat ini. Gunakan perintah berikut dan ganti *us-east-1* dengan kode Wilayah tempat Anda menggunakan sumber daya:

   ```
   $ REGION=us-east-1
   ```

2. Script tester hanya tersedia melalui AWS Systems Manager (SSM). Untuk memulai shell interaktif pada instance host tester, kueri host InstanceId.
3. Gunakan perintah berikut untuk memulai sesi Anda untuk skrip tester:

   ```
   aws ssm start-session
     --region $REGION
     --document-name AWS-StartInteractiveCommand
     --parameters command="cd /home/ssm-user/py_tester && bash -l"
     --target $(aws ec2 describe-instances
       --region $REGION
       --filters "Name=tag:Name,Values=Driver-GuardDutyTester"
       --query "Reservations[].Instances[?State.Name=='running'].InstanceId"
       --output text)
   ```

Bagian B - Menghasilkan temuan

Skrip tester adalah Python-based program yang secara dinamis membangun skrip bash untuk menghasilkan temuan berdasarkan masukan Anda. Anda memiliki fleksibilitas untuk menghasilkan temuan berdasarkan satu atau lebih jenis AWS sumber daya, rencana GuardDuty perlindungan, Tujuan Ancaman (taktik)Sumber data dasar, atauthe section called “GuardDuty temuan skrip tester dapat menghasilkan”.

Gunakan contoh perintah berikut sebagai referensi, dan jalankan satu atau beberapa perintah untuk menghasilkan temuan yang ingin Anda jelajahi:

```
python3 guardduty_tester.py
```

```
python3 guardduty_tester.py --all
python3 guardduty_tester.py --s3
python3 guardduty_tester.py --tactics discovery
python3 guardduty_tester.py --ec2 --eks --tactics backdoor policy execution
python3 guardduty_tester.py --eks --runtime only
python3 guardduty_tester.py --ec2 --runtime only --tactics impact
python3 guardduty_tester.py --log-source dns vpc-flowlogs
python3 guardduty_tester.py --finding 'CryptoCurrency:EC2/BitcoinTool.B!DNS'
```

Untuk informasi lebih lanjut tentang parameter yang valid, Anda dapat menjalankan perintah bantuan berikut:

```
python3 guardduty_tester.py --help
```

Bagian C - Tinjau temuan yang dihasilkan

Pilih metode yang disukai untuk melihat temuan yang dihasilkan di akun Anda.

GuardDuty console

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Temuan.
3. Dari tabel temuan, pilih temuan yang ingin Anda lihat detailnya. Ini akan membuka panel detail temuan. Untuk informasi, lihat Memahami dan menghasilkan GuardDuty temuan Amazon.
4. Jika Anda ingin memfilter temuan ini, gunakan kunci dan nilai tag sumber daya. Misalnya, untuk memfilter temuan yang dihasilkan untuk instans Amazon EC2, gunakan**`CreatedBy`**: **`GuardDuty Test Script`** tag key:value pair untuk kunci tag Instance dan kunci tag Instance.

API

- Jalankan ListFindingsuntuk melihat temuan untuk ID detektor tertentu. Anda dapat menentukan parameter untuk memfilter temuan.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

AWS CLI

- Jalankan AWS CLI perintah berikut untuk melihat temuan yang dihasilkan dan ganti *us-east-1* dan *12abc34d567e8fa901bc2d34EXAMPLE* dengan nilai yang sesuai:

```
aws guardduty list-findings --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34EXAMPLE
```

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

  Untuk informasi selengkapnya tentang parameter yang dapat Anda gunakan untuk memfilter temuan, lihat daftar-temuan di Referensi AWS CLI Perintah.

Langkah 4 - Bersihkan sumber daya AWS tes

Pengaturan tingkat akun dan pembaruan status konfigurasi lainnya yang dibuat selama Langkah 3 - Jalankan skrip penguji kembali ke keadaan semula saat skrip penguji selesai.

Setelah Anda menjalankan skrip tester, Anda dapat memilih untuk membersihkan sumber daya AWS pengujian. Anda dapat memilih untuk melakukan ini dengan menggunakan salah satu metode berikut:

- Jalankan perintah berikut:

```
cdk destroy
```

- Hapus CloudFormation tumpukan dengan nama GuardDutyTesterStack. Untuk selengkapnya tentang langkah-langkah, lihat Menghapus tumpukan di CloudFormation konsol.

Memecahkan masalah umum

GuardDuty telah mengidentifikasi masalah umum dan merekomendasikan langkah-langkah pemecahan masalah:

- `Cloud assembly schema version mismatch`— Perbarui AWS CDK CLI ke versi yang kompatibel dengan versi perakitan cloud yang diperlukan, atau ke versi terbaru yang tersedia. Untuk informasi selengkapnya, lihat AWS CDK Kompatibilitas CLI.

- `Docker permission denied`— Tambahkan pengguna akun khusus ke docker atau docker-users sehingga akun khusus dapat menjalankan perintah. Untuk informasi selengkapnya tentang langkah-langkah, lihat opsi soket Daemon.
- `Your requested instance type is not supported in your requested Availability Zone`— Beberapa zona Availability tidak mendukung jenis instans tertentu. Untuk mengidentifikasi zona ketersediaan mana yang mendukung jenis instans pilihan Anda dan mencoba kembali untuk menerapkan AWS sumber daya, lakukan langkah-langkah berikut:

  1. Pilih metode yang disukai untuk menentukan zona Ketersediaan mana yang mendukung jenis instans Anda:

     Console

     Untuk mengidentifikasi Availability zone yang mendukung tipe instans pilihan

     1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
     2. Dengan menggunakan pemilih AWS Region di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin meluncurkan instance.
     3. Di panel navigasi, di bawah Instance, pilih Jenis Instance.
     4. Dari tabel tipe Instance, pilih jenis instance yang disukai.
     5. Di bawah Jaringan, lihat Wilayah yang tercantum di bawah Availability zone.

        Berdasarkan informasi ini, Anda mungkin perlu memilih Wilayah baru tempat Anda dapat menyebarkan sumber daya.

     AWS CLI

     Jalankan perintah berikut untuk melihat daftar Availability zone. Pastikan untuk menentukan jenis instans pilihan Anda dan Region (*us-east-1*).

     ```
     aws ec2 describe-instance-type-offerings --location-type availability-zone  --
     filters Name=instance-type,Values=Preferred instance type --region us-east-1 --
     output table
     ```

     Untuk informasi selengkapnya tentang perintah ini, lihat describe-instance-type-offerings di Command Reference.AWS CLI

Saat menjalankan perintah ini, jika Anda menerima kesalahan, pastikan Anda menggunakan versi terbaru AWS CLI. Untuk informasi selengkapnya, lihat Pemecahan Masalah di AWS Command Line Interface Panduan Pengguna.

2. Coba gunakan sumber AWS daya lagi dan tentukan zona Ketersediaan yang mendukung jenis instans pilihan Anda.

   Untuk mencoba kembali menyebarkan sumber daya AWS

   1. Siapkan Region default dalam `bin/cdk-gd-tester.ts` file.
   2. Untuk menentukan zona ketersediaan, buka `amazon-guardduty-tester/lib/common/network/vpc.ts` file.
   3. Dalam file ini, ganti `maxAzs: 2,` dengan `availabilityZones: ['us-east-1a', 'us-east-1c'],` tempat Anda harus menentukan zona Ketersediaan untuk jenis instans Anda.
   4. Lanjutkan dengan langkah-langkah yang tersisa di bawahLangkah-langkah untuk menyebarkan sumber daya AWS.

Melihat temuan yang dihasilkan di GuardDuty konsol

Ketika GuardDuty mendeteksi aktivitas yang cocok dengan pola masalah keamanan, GuardDuty menghasilkan temuan. Temuan ini terkait dengan jenis sumber daya yang mungkin telah dikompromikan selama aktivitas ini. Anda dapat melihat detail yang terkait dengan setiap temuan yang GuardDuty dihasilkan.

Jika Anda menggunakan akun GuardDuty administrator, Anda dapat melihat temuan yang dihasilkan atas nama akun anggota. Namun, akun anggota dapat melihat temuan yang dihasilkan di akun mereka sendiri. Akun anggota tidak dapat melihat temuan yang dihasilkan untuk akun anggota lain.

Langkah-langkah untuk melihat temuan di GuardDuty konsol

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi kiri, pilih Temuan.

   GuardDuty menampilkan temuan dalam format tabular. Secara default, tabel ini diurutkan dalam urutan menurun berdasarkan nilai kolom Ter akhir dilihat, menampilkan temuan terbaru di bagian atas.

Temuan dengan ikon pedang

()

mewakili penemuan urutan serangan.

3. Untuk melihat detail yang terkait dengan temuan, pilih Judul nya. Ini akan membuka panel samping rincian temuan. Untuk menemukan urutan serangan, panel samping ini menyertakan versi ringkasan dari urutan serangan, dan untuk memperluas tampilan ini, pilih Lihat detail.

   Untuk informasi tentang bidang yang tercantum di panel samping ini, lihatDetail temuan.

4. (Opsional) untuk mengunduh pencarian JSON

   a. Pilih temuan, lalu pilih menu T indakan.

   b. Pada menu Tindakan, pilih Lihat dan ekspor JSON.

   c. Pada jendela Findings JSON, pilih Download.

> **Note**
>
> Dalam beberapa kasus, GuardDuty menjadi sadar bahwa temuan tertentu adalah positif palsu setelah mereka dihasilkan. GuardDuty menyediakan bidang Keyakinan dalam JSON temuan, dan menetapkan nilainya menjadi nol. Dengan cara GuardDuty ini Anda tahu bahwa Anda dapat dengan aman mengabaikan temuan tersebut.
> Temuan tanpa bidang Keyakinan tidak dianggap positif palsu.

Menavigasi halaman Temuan

Bagian ini memberikan informasi penting tentang berbagai elemen pada halaman Temuan. Ini akan membantu Anda menganalisis temuan yang dihasilkan untuk analisis dan respons ancaman.

Daftar berikut menjelaskan elemen halaman Temuan yang akan membantu Anda lebih memahami temuan yang dihasilkan:

- Jenis ancaman:

  Jenis ancaman mencakup GuardDuty temuan individu dan temuan urutan serangan. Secara default, halaman menampilkan Semua temuan.

Untuk memfilter tampilan tabel temuan, pada menu Jenis ancaman, pilih salah satu opsi — Hanya temuan urutan serangan atau Temuan individu saja.

- Kolom Sumber Daya dan Hitungan:

  Kol om Sumber daya dalam tabel temuan menunjukkan nama AWS sumber daya yang berpotensi dikompromikan. Untuk penemuan urutan serangan, kolom ini menunjukkan jumlah AWS sumber daya yang berpotensi dikompromikan. Untuk melihat nama sumber daya, pilih nomor di bawah kolom Resource.

  Kolom Hitungan menunjukkan berapa kali GuardDuty mengamati temuan tertentu. Ketika GuardDuty mendeteksi bahwa aktivitas yang cocok dengan masalah keamanan yang diidentifikasi sebelumnya, itu menambah jumlah untuk temuan spesifik tersebut. Untuk penemuan urutan serangan, nilai kolom ini menunjukkan jumlah total sinyal dan temuan yang terlibat dalam pembuatan temuan.

- Menyortir temuan berdasarkan kolom tabel:

  Jika ada panah di sebelah header kolom, maka Anda dapat mengurutkan tabel temuan berdasarkan kolom. Pilih header kolom untuk mengurutkan temuan dalam urutan peningkatan atau penurunan nilai di kolom itu.

- Penyaringan temuan:

  Berdasarkan atribut properti tertentu, seperti `Account ID` dan`Resource type`, Anda dapat memfilter tabel temuan lebih lanjut. Untuk informasi tentang jenis filter yang dapat Anda gunakan, lihatPenyaringan temuan GuardDuty .

- Status dan aturan tersimpan:

  Menu Status mencakup dua nilai - Cur rent dan Archives. Tampilan default adalah Temuan terkini dalam tabel.

  Ketika Anda tidak lagi GuardDuty ingin menghasilkan temuan yang cocok dengan kriteria tertentu, Anda dapat menekan temuan itu. GuardDuty Arsipkan temuan itu. Ketika GuardDuty mendeteksi temuan ini lagi, Anda tidak akan diberitahu tentang pengamatan ini. Untuk melihat temuan yang diarsipkan secara khusus, pada menu Status, pilih Diarsipkan.

  Aturan tersimpan adalah fitur yang membantu Anda memfilter dan mengambil tindakan secara otomatis pada temuan yang sesuai dengan kriteria tertentu. Tindakan dapat mencakup pengarsipan temuan atau menekannya dari pemberitahuan di masa mendatang.

Untuk informasi selengkapnya, lihat Aturan penekanan.

Tingkat keparahan GuardDuty temuan

Setiap GuardDuty temuan memiliki tingkat keparahan dan nilai yang ditetapkan yang mencerminkan potensi risiko temuan terhadap lingkungan Anda, seperti yang ditentukan oleh teknisi keamanan kami. Nilai tingkat keparahan dapat berada di mana saja dalam kisaran 1,0 hingga 10,0, dengan nilai yang lebih tinggi menunjukkan risiko keamanan yang lebih besar. Untuk membantu Anda menentukan respons terhadap masalah keamanan potensial yang disorot oleh temuan, pisahkan kisaran GuardDuty ini menjadi tingkat keparahan Kritis , Tinggi, Sedang, dan R endah.

Temuan jenis tertentu mungkin memiliki tingkat keparahan yang berbeda tergantung pada konteks khusus untuk temuan tersebut. Untuk melihat daftar gabungan tingkat keparahan default untuk semua jenis GuardDuty temuan, lihatGuardDuty jenis temuan aktif.

Bagian berikut menjelaskan tingkat keparahan yang ditentukan untuk tem GuardDuty uan.

Topik

- Tingkat keparahan kritis
- Tingkat keparahan tinggi
- Tingkat keparahan sedang
- Tingkat keparahan rendah

Tingkat keparahan kritis

Rentang nilai: 9,0 - 10,0

Deskripsi: Tingkat keparahan kritis menunjukkan bahwa urutan serangan mungkin sedang berlangsung atau baru-baru ini terjadi. Satu atau lebih AWS sumber daya, seperti kredentif masuk pengguna IAM dan bucket Amazon S3, berpotensi dikompromikan atau mungkin telah dikompromikan.

Rekomendasi: GuardDuty merekomendasikan agar Anda memprioritaskan triaging dan memperbaiki semua temuan tingkat keparahan kritis karena masalah ini dapat menjadi bagian dari serangan ransomware dan dapat meningkat kapan saja. Lihat detail tentang sumber daya yang terlibat dan mulai menangani masalah keamanan. Untuk informasi selengkapnya, lihat Mengatasi temuan.

Tingkat keparahan tinggi

Kisaran nilai: 7,0 - 8,9

Deskripsi: Tingkat keparahan tinggi menunjukkan bahwa sumber daya yang dimaksud (instans Amazon EC2 atau sekumpulan kredentif masuk pengguna IAM) dikompromikan dan secara aktif digunakan untuk tujuan yang tidak sah.

Rekomendasi: GuardDuty merekomendasikan agar Anda memperlakukan masalah keamanan pencarian tingkat keparahan tinggi sebagai prioritas dan mengambil langkah-langkah perbaikan segera untuk mencegah penggunaan sumber daya Anda secara tidak sah lebih lanjut. Misalnya, bersihkan instans Amazon EC2 Anda atau hentikan, atau putar kredentif IAM. Ikuti langkah-langkah Mengatasi temuan untuk memperbaiki temuan.

Tingkat keparahan sedang

Rentang nilai: 4,0 - 6,9

Deskripsi: Tingkat keparahan sedang menunjukkan aktivitas mencurigakan yang menyimpang dari perilaku yang diamati secara normal dan, tergantung pada kasus penggunaan Anda, mungkin merupakan indikasi adanya kompromi sumber daya.

Rekomendasi: GuardDuty merekomendasikan untuk menyelidiki sumber daya yang berpotensi terkena dampak sesegera mungkin. Langkah-langkah remediasi akan bervariasi menurut sumber daya dan keluarga yang ditemukan. Pendekatan yang mapan adalah bagi Anda untuk mengonfirmasi bahwa aktivitas tersebut diotorisasi dan konsisten dengan kasus penggunaan Anda. Jika Anda tidak dapat mengidentifikasi penyebabnya, atau mengonfirmasi bahwa aktivitas telah diotorisasi, Anda harus mempertimbangkan sumber daya yang dikompromikan. Ikuti langkah-langkah Mengatasi temuan untuk memperbaiki temuan.

Berikut adalah beberapa hal yang perlu dipertimbangkan ketika meninjau temuan tingkat menengah:

- Periksa apakah pengguna yang berwenang telah menginstal perangkat lunak baru yang mengubah perilaku sumber daya (misalnya, mengizinkan lalu lintas yang lebih tinggi dari biasanya, atau mengaktifkan komunikasi pada port baru).
- Periksa apakah pengguna yang berwenang mengubah pengaturan bidang kontrol, misalnya, mengubah pengaturan grup keamanan.
- Jalankan pemindaian anti-virus pada sumber daya yang bersangkutan untuk mendeteksi perangkat lunak yang tidak sah.

- Verifikasi izin yang terlampir pada IAM role, pengguna, grup, atau set kredensial yang bersangkutan. Ini mungkin harus diubah atau diputar.

Tingkat keparahan rendah

Rentang nilai: 1,0 - 3,9

Deskripsi: Tingkat keparahan rendah menunjukkan upaya aktivitas mencurigakan yang tidak membahayakan lingkungan Anda, misalnya, pemindaian port atau upaya intrusi yang gagal.

Rekomendasi: Tidak ada tindakan yang direkomendasikan segera, tetapi ada baiknya mencatat informasi ini karena mungkin menunjukkan seseorang sedang mencari titik lemah di lingkungan Anda.

Detail temuan

Di GuardDuty konsol Amazon, Anda dapat melihat detail pencarian di bagian ringkasan pencarian. Detail menemukan bervariasi berdasarkan jenis temuan.

Ada dua detail utama yang menentukan jenis informasi apa yang tersedia untuk temuan apa pun. Yang pertama adalah jenis sumber daya, yang dapat berupa `InstanceAccessKey`,`S3Bucket`,`S3Object`,`Kubernetes cluster`,`ECS cluster`,`Container`,`RDSDBInstance`,`RDSLimitlessDB`, atau`Lambda`. Detail kedua yang menentukan informasi temuan adalah Peran Sumber Daya. Peran sumber daya bisa`Target`, artinya sumber daya adalah target aktivitas yang mencurigakan. Untuk temuan tipe instans, peran sumber daya juga dapat menjadi `Actor`, yang berarti bahwa sumber daya Anda adalah aktor yang melakukan aktivitas mencurigakan. Topik ini menjelaskan beberapa detail umum yang tersedia untuk temuan. Untuk the section called “Jenis penemuan Runtime Monitoring” danPerlindungan Malware untuk tipe pencarian S3, peran sumber daya tidak diisi.

Topik

- Menemukan ikhtisar
- Sumber daya
- Detail pencarian urutan serangan
- Aturan Deteksi Kustom menemukan detail
- Rincian pengguna database RDS (DB)

- Detail temuan Pemantauan Runtime
- Detail pemindaian volume EBS
- Perlindungan Malware untuk detail pencarian EC2
- Detail temuan Perlindungan Malware untuk S3
- Tindakan
- Aktor atau Target
- Detail geolokasi
- Informasi tambahan
- Bukti
- Perilaku anomali

Menemukan ikhtisar

Bagian Ikhtisar temuan berisi fitur pengenal paling dasar dari temuan, termasuk informasi berikut:

- ID Akun — ID AWS akun tempat aktivitas berlangsung yang mendorong GuardDuty untuk menghasilkan temuan ini.
- Hitung — Berapa kali GuardDuty telah mengumpulkan aktivitas yang cocok dengan pola ini dengan ID temuan ini.
- Dibuat pada — Waktu dan tanggal ketika temuan ini pertama kali dibuat. Jika nilai ini berbeda dari Diperbarui pada, ini menunjukkan bahwa aktivitas tersebut telah terjadi beberapa kali dan merupakan masalah yang sedang berlangsung.

> **Note**
>
> Stempel waktu untuk temuan di GuardDuty konsol muncul di zona waktu lokal Anda, sementara ekspor JSON dan output CLI menampilkan stempel waktu di UTC.

- Finding ID — Pengidentifikasi unik untuk jenis temuan ini dan kumpulan parameter. Kejadian baru dari aktivitas yang cocok dengan pola ini akan digabungkan ke ID yang sama.
- Tipe temuan – String berformat yang mewakili tipe aktivitas yang memicu temuan. Untuk informasi selengkapnya, lihat GuardDuty menemukan format.
- Wilayah — AWS Wilayah di mana temuan itu dihasilkan. Untuk informasi selengkapnya tentang Wilayah yang didukung, lihat Wilayah dan titik akhir

- ID Sumber Daya — ID AWS sumber daya tempat aktivitas berlangsung yang mendorong GuardDuty untuk menghasilkan temuan ini.
- ID Pindai — Berlaku untuk temuan saat Perlindungan GuardDuty Malware untuk EC2 diaktifkan, ini adalah pengidentifikasi pemindaian malware yang berjalan pada volume EBS yang melekat pada instans EC2 atau beban kerja kontainer yang berpotensi dikompromikan. Untuk informasi selengkapnya, lihat Perlindungan Malware untuk detail pencarian EC2.
- Keparahan — Tingkat keparahan yang ditetapkan temuan baik Kritis, Tinggi, Sedang, atau Rendah. Untuk informasi selengkapnya, lihat Tingkat keparahan temuan.
- Diperbarui di — Terakhir kali temuan ini diperbarui dengan aktivitas baru yang cocok dengan pola yang mendorong GuardDuty untuk menghasilkan temuan ini.

Sumber daya

Sumber daya yang terpengaruh memberikan rincian tentang AWS sumber daya yang ditargetkan oleh aktivitas inisiasi. Informasi yang tersedia bervariasi berdasarkan tipe sumber daya dan tipe tindakan.

Peran sumber daya — Peran AWS sumber daya yang memulai temuan. Nilai ini bisa TARGET atau ACTOR, dan mewakili apakah sumber daya Anda adalah target aktivitas mencurigakan atau aktor yang melakukan aktivitas mencurigakan.

Jenis sumber daya — Jenis sumber daya yang terpengaruh. Jika beberapa sumber daya terlibat, temuan dapat mencakup beberapa jenis sumber daya. Jenis sumber daya adalah Instance,, S3Bucket AccessKey, S3Object,, ECSCluster, Container, RDSDBInstance KubernetesCluster, RDSLimitlessDB, dan Lambda. Tergantung tipe sumber dayanya, detail temuan yang berbeda tersedia. Pilih tab opsi sumber daya untuk mempelajari detail yang tersedia untuk sumber daya tersebut.

Instance

Detail contoh:

> **Note**
>
> Beberapa detail instance mungkin hilang jika instance telah dihentikan atau jika pemanggilan API yang mendasarinya berasal dari instans EC2 di Wilayah lain saat melakukan panggilan API Lintas wilayah.

- ID Instance — ID dari instans EC2 yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- Jenis Instance — Jenis instans EC2 yang terlibat dalam temuan.
- Waktu Peluncuran - Waktu dan tanggal peluncuran instans.
- Outpost ARN — Nama Sumber Daya Amazon (ARN) dari. AWS Outposts Hanya berlaku untuk AWS Outposts instance. Untuk informasi lebih lanjut, lihat Apa itu AWS Outposts? di Panduan Pengguna untuk rak Outposts.
- Nama Grup Keamanan – Nama Grup Keamanan yang melekat pada instans yang terlibat.
- ID Grup Keamanan – ID grup keamanan yang melekat pada instans yang terlibat.
- Status instans – Status instans yang ditargetkan saat ini.
- Availability Zone – Availability Zone AWS Region tempat instans yang terlibat berada.
- ID Image – ID dari Amazon Machine Image yang digunakan untuk membangun instans yang terlibat dalam aktivitas.
- Deskripsi Image – Deskripsi ID Amazon Machine Image yang digunakan untuk membangun instans yang terlibat dalam aktivitas.
- Tanda – Daftar tanda yang melekat pada sumber daya ini, tercantum dalam format `key:value`.

AccessKey

Akses Detail Kunci:

- ID kunci akses — ID kunci akses pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- Principal ID — ID utama pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- Jenis pengguna — Jenis pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.
- Nama pengguna — Nama pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.

S3Bucket

Detail ember Amazon S3:

- Nama – Nama bucket yang terlibat dalam temuan.

- ARN – ARN bucket yang terlibat dalam temuan.
- Pemilik – ID pengguna resmi dari pengguna yang memiliki bucket yang terlibat dalam temuan. Untuk informasi selengkapnya tentang ID pengguna resmi, lihat pengenal akun AWS.
- Tipe – Tipe temuan bucket, dapat berupa Tujuan atau Sumber.
- Enkripsi sisi server default — Detail enkripsi untuk bucket.
- Tag Bucket — Daftar tag yang dilampirkan pada sumber daya ini, tercantum dalam format`key:value`.
- Izin Efektif – Evaluasi dari semua izin dan kebijakan efektif pada bucket yang menunjukkan apakah bucket yang terlibat diekspos secara publik. Nilai bisa publik atau tidak publik.

S3Object

- Detail objek S3 - Termasuk informasi berikut tentang objek S3 yang dipindai:
  - ARN - Nama Sumber Daya Amazon (ARN) dari objek S3 yang dipindai.
  - Kunci — Nama yang ditetapkan ke file saat dibuat di bucket S3.
  - Id Versi — Bila Anda telah mengaktifkan versi bucket, bidang ini menunjukkan Id versi yang terkait dengan versi terbaru dari objek S3 yang dipindai. Untuk informasi selengkapnya, lihat Menggunakan pembuatan versi di bucket S3 di Panduan Pengguna Amazon S3.
  - ETag - Merupakan versi spesifik dari objek S3 yang dipindai.
  - Hash — Hash dari ancaman yang terdeteksi dalam temuan ini.
- Detail bucket S3 — Termasuk informasi berikut tentang bucket Amazon S3 yang terkait dengan objek S3 yang dipindai:
  - Nama - Menunjukkan nama bucket S3 yang berisi objek.
  - ARN - Nama Sumber Daya Amazon (ARN) dari ember S3.
- Pemilik — Id Canonical dari pemilik bucket S3.

EKSCluster

Detail klaster Kubernetes:

- Nama — Nama cluster Kubernetes.
- ARN — ARN yang mengidentifikasi cluster.
- Created At — Waktu dan tanggal ketika cluster ini dibuat.

> **Note**
>
> Stempel waktu untuk temuan di GuardDuty konsol muncul di zona waktu lokal Anda, sementara ekspor JSON dan output CLI menampilkan stempel waktu di UTC.

- ID VPC — ID VPC yang terkait dengan cluster Anda.
- Status — Status cluster saat ini.
- Tag — Metadata yang Anda terapkan ke cluster untuk membantu Anda mengkategorikan dan mengaturnya. Setiap tag terdiri dari kunci dan nilai opsional, yang tercantum dalam format`key:value`. Anda bisa menentukan kunci dan nilai.

  Tag cluster tidak menyebar ke sumber daya lain yang terkait dengan cluster.

Detail beban kerja Kubernetes:

- Jenis - Jenis beban kerja Kubernetes, seperti pod, deployment, dan job.
- Nama — Nama beban kerja Kubernetes.
- Uid — ID unik dari beban kerja Kubernetes.
- Dibuat pada - Waktu dan tanggal ketika beban kerja ini dibuat.
- Label — Pasangan nilai kunci yang melekat pada beban kerja Kubernetes.
- Container — Detail kontainer yang berjalan sebagai bagian dari beban kerja Kubernetes.
- Namespace — Beban kerja milik namespace Kubernetes ini.
- Volume — Volume yang digunakan oleh beban kerja Kubernetes.
  - Jalur host - Merupakan file atau direktori yang sudah ada sebelumnya di mesin host tempat volume dipetakan.
  - Nama — Nama volume.
- konteks keamanan pod — Mendefinisikan pengaturan privilege dan acess control untuk semua kontainer dalam sebuah pod.
- Jaringan host — Setel ke `true` jika pod disertakan dalam beban kerja Kubernetes.

Detail pengguna Kubernetes:

- Grup - Kubernetes RBAC (kontrol berbasis akses peran) kelompok pengguna yang terlibat dalam aktivitas yang menghasilkan temuan.

- ID — ID unik dari pengguna Kubernetes.
- Nama pengguna — Nama pengguna Kubernetes yang terlibat dalam aktivitas yang menghasilkan temuan.
- Nama sesi — Entitas yang mengambil peran IAM dengan izin Kubernetes RBAC.

ECSCluster

Rincian cluster ECS:

- ARN — ARN yang mengidentifikasi cluster.
- Nama — Nama cluster.
- Status — Status cluster saat ini.
- Jumlah layanan aktif — Jumlah layanan yang berjalan di cluster dalam suatu `ACTIVE` keadaan. Anda dapat melihat layanan ini dengan ListServices
- Jumlah instans kontainer terdaftar — Jumlah instance kontainer yang terdaftar ke dalam klaster. Ini termasuk instance kontainer di keduanya `ACTIVE` dan `DRAINING` status.
- Menjalankan tugas menghitung — Jumlah tugas di cluster yang berada dalam `RUNNING` status.
- Tag — Metadata yang Anda terapkan ke cluster untuk membantu Anda mengkategorikan dan mengaturnya. Setiap tag terdiri dari kunci dan nilai opsional, yang tercantum dalam format`key:value`. Anda bisa menentukan kunci dan nilai.
- Kontainer — Detail tentang wadah yang terkait dengan tugas:
  - Nama kontainer — Nama wadah.
  - Gambar kontainer — Gambar wadah.
- Detail tugas — Detail tugas dalam sebuah cluster.
  - ARN — Nama Sumber Daya Amazon (ARN) dari tugas tersebut.
  - Definisi ARN — Nama Sumber Daya Amazon (ARN) dari definisi tugas yang membuat tugas.
  - Versi - Penghitung versi untuk tugas tersebut.
  - Tugas dibuat di — Stempel waktu Unix saat tugas dibuat.
  - Tugas dimulai pada — Stempel waktu Unix saat tugas dimulai.
  - Tugas dimulai oleh — Tag yang ditentukan saat tugas dimulai.

Container

Detail kontainer:

- Container runtime — Container runtime (seperti `docker` atau`containerd`) yang digunakan untuk menjalankan container.
- ID - ID instance kontainer atau entri ARN lengkap untuk instance kontainer.
- Nama — Nama wadah.
- Gambar - Gambar dari contoh kontainer.
- Volume mount — Daftar dudukan volume kontainer. Sebuah wadah dapat memasang volume di bawah sistem file-nya.
- Konteks keamanan — Konteks keamanan kontainer mendefinisikan hak istimewa dan pengaturan kontrol akses untuk kontainer.
- Detail proses — Menjelaskan detail proses yang terkait dengan temuan.

RDSDBInstance

Rincian RDSDBInstance:

> **Note**
>
> Sumber daya ini tersedia dalam temuan Perlindungan RDS yang terkait dengan instance database.

- Database Instance ID — Pengidentifikasi yang terkait dengan instance database yang terlibat dalam GuardDuty temuan.
- Engine — Nama mesin database dari instance database yang terlibat dalam temuan. Nilai yang mungkin adalah Aurora atau MySQL-Compatible Aurora. PostgreSQL-Compatible
- Versi mesin — Versi mesin database yang terlibat dalam GuardDuty temuan.
- Database cluster ID — Pengidentifikasi cluster database yang berisi ID instance database yang terlibat dalam GuardDuty temuan.
- Database instance ARN — ARN yang mengidentifikasi instance database yang terlibat dalam temuan. GuardDuty

RDSLimitlessDB

Rincian RDSLimitlessDB:

Sumber daya ini tersedia dalam temuan Perlindungan RDS yang terkait dengan versi mesin yang didukung dari Limitless Database.

- Pengidentifikasi grup shard DB — Nama yang terkait dengan grup shard DB Limitless.
- ID sumber daya grup shard DB — Pengidentifikasi sumber daya dari grup pecahan DB dalam DB Limitless.
- Grup pecahan DB ARN — Nama Sumber Daya Amazon (ARN) yang mengidentifikasi grup pecahan DB.
- Engine — Pengidentifikasi Limitless DB yang terlibat dalam temuan.
- Versi mesin — Versi mesin Limitless DB.
- DB cluster identifier — Nama cluster database yang merupakan bagian dari Limitless DB.

Untuk informasi tentang pengguna dan detail otentikasi dari database yang berpotensi terkena dampak, lihat. Rincian pengguna database RDS (DB)

Lambda

Detail fungsi Lambda

- Nama fungsi — Nama fungsi Lambda yang terlibat dalam temuan.
- Versi fungsi — Versi fungsi Lambda yang terlibat dalam temuan.
- Deskripsi fungsi — Deskripsi fungsi Lambda yang terlibat dalam temuan.
- Fungsi ARN — Nama Sumber Daya Amazon (ARN) dari fungsi Lambda yang terlibat dalam temuan.
- ID Revisi — ID revisi versi fungsi Lambda.
- Peran — Peran eksekusi fungsi Lambda yang terlibat dalam temuan.
- Konfigurasi VPC - Konfigurasi VPC Amazon, termasuk ID VPC, grup keamanan, dan ID subnet yang terkait dengan fungsi Lambda Anda.
  - ID VPC — ID VPC Amazon yang terkait dengan fungsi Lambda yang terlibat dalam temuan.
  - ID Subnet — ID subnet yang terkait dengan fungsi Lambda Anda.
  - Grup Keamanan — Kelompok keamanan yang melekat pada fungsi Lambda yang terlibat. Ini termasuk nama grup keamanan dan ID grup.

- Tag — Daftar tag yang dilampirkan ke sumber daya ini, tercantum dalam format`key: value` pasangan.

Detail pencarian urutan serangan

GuardDuty memberikan detail untuk setiap temuan yang dihasilkannya di akun Anda. Detail ini membantu Anda memahami alasan di balik temuan tersebut. Bagian ini berfokus pada detail yang terkait dengan[Jenis pencarian urutan serangan](). Ini termasuk wawasan seperti sumber daya yang berpotensi terkena dampak, garis waktu peristiwa, indikator, sinyal, dan titik akhir yang terlibat dalam temuan.

Untuk melihat detail yang terkait dengan sinyal yang merupakan GuardDuty temuan, lihat bagian terkait di halaman ini.

Di GuardDuty konsol, saat Anda memilih pencarian urutan serangan, panel samping detail dibagi menjadi tab berikut:

- Ikhtisar — Memberikan tampilan ringkas tentang detail urutan serangan, termasuk sinyal, taktik MITRE, dan sumber daya yang berpotensi terkena dampak.
- Sinyal — Menampilkan garis waktu peristiwa yang terlibat dalam urutan serangan.
- Sumber Daya — Memberikan informasi tentang sumber daya yang berpotensi terkena dampak, atau sumber daya yang berpotensi berisiko.

Daftar berikut memberikan deskripsi yang terkait dengan rincian pencarian urutan serangan.

Sinyal

Sinyal bisa berupa aktivitas API atau temuan yang GuardDuty digunakan untuk mendeteksi temuan urutan serangan. GuardDuty menganggap sinyal lemah yang tidak menampilkan diri sebagai ancaman yang jelas, menyatukannya, dan berkorelasi dengan temuan yang dihasilkan secara individual. Untuk konteks lebih lanjut, tab Sinyal menyediakan garis waktu sinyal, seperti yang diamati oleh GuardDuty.

Setiap sinyal, yang merupakan GuardDuty temuan, memiliki tingkat keparahan dan nilai yang ditetapkan untuk itu sendiri. Di GuardDuty konsol, Anda dapat memilih setiap sinyal untuk melihat detail terkait.

Aktor

Memberikan rincian tentang aktor ancaman dalam urutan serangan. Untuk informasi selengkapnya, lihat Referensi Aktor di Amazon GuardDuty API.

Titik akhir

Memberikan rincian tentang titik akhir jaringan yang digunakan dalam urutan serangan ini. Untuk informasi selengkapnya, lihat NetworkEndpointdi Referensi Amazon GuardDuty API. Untuk informasi tentang cara GuardDuty menentukan lokasi, lihatDetail geolokasi.

Indikator

Termasuk data yang diamati yang cocok dengan pola masalah keamanan. Data ini menentukan mengapa GuardDuty ada indikasi aktivitas yang berpotensi mencurigakan. Misalnya, ketika nama indikatornya`HIGH_RISK_API`, ini menunjukkan tindakan yang biasa digunakan oleh pelaku ancaman, atau tindakan sensitif yang dapat menyebabkan dampak potensial pada Akun AWS, seperti mengakses kredensil atau memodifikasi sumber daya.

Tabel berikut mencakup daftar indikator potensial dan deskripsinya:

Nama indikator	Deskripsi
`ATTACK_TACTIC`	Taktik MITRE yang digunakan oleh aktor ancaman dalam urutan serangan. Contohnya termasuk Discovery and Impact.
`ATTACK_TECHNIQUE`	Teknik MITRE yang digunakan oleh aktor ancaman dalam urutan serangan. Contohnya termasuk mendapatkan akses ke sumber daya dan menggunakannya dengan cara yang tidak diinginkan, dan mengeksploitasi kerentanan.
`CRYPTOMINING_DOMAIN`	Menunjukkan nama domain yang terkait dengan kolam atau infrastruktur penambangan cryptocurrency. Misalnya, kueri atau koneksi DNS ke domain ini dari container atau lingkungan Kubernetes dapat mengindikasikan aktivitas cryptomining yang tidak sah.
`CRYPTOMINING_IP`	Menunjukkan alamat IP yang terkait dengan kolam atau infrastruktur penambangan cryptocurrency. Misalnya, koneksi ke alamat-alamat ini dari container atau lingkungan Kubernetes dapat mengindikasikan aktivitas cryptomining yang tidak sah.

Nama indikator	Deskripsi
`CRYPTOMINING_PROCESS`	Menunjukkan proses yang diidentifikasi sebagai perangkat lunak penambangan cryptocurrency yang berjalan di dalam wadah atau lingkungan Kubernetes. Misalnya, proses ini dapat mengkonsumsi sumber daya CPU yang berlebihan.
`HIGH_RISK_API`	AWS API yang menyertakan Layanan AWS nama dan `eventName` menunjukkan tindakan yang biasa digunakan oleh pelaku ancaman, atau merupakan tindakan sensitif yang dapat menyebabkan dampak potensial pada Akun AWS, seperti akses kredensi atau modifikasi sumber daya.
`MALICIOUS_DOMAIN`	Menunjukkan nama domain dengan dugaan intelijen ancaman yang menunjukkan niat jahat. Misalnya, ini termasuk server perintah dan kontrol (C&C), situs distribusi malware, atau domain phishing yang dihubungi dari container atau lingkungan Kubernetes.
`MALICIOUS_FILE`	Menunjukkan file yang dicurigai berbahaya berdasarkan kecerdasan ancaman atau analisis perilaku. Misalnya, ini termasuk binari malware yang dikenal, skrip berbahaya, atau executable yang tidak sah.
`MALICIOUS_IP`	Alamat IP telah mengkonfirmasi intelijen ancaman yang menunjukkan niat jahat.
`MALICIOUS_PACKAGE`	Menunjukkan bahwa sumber daya yang terlibat dalam urutan serangan berisi paket perangkat lunak yang diidentifikasi sebagai berbahaya. Nilai indikator termasuk pengidentifikasi paket berbahaya menggunakan penunjukan OSV (MAL-*) yang terkait dengan paket yang terdeteksi.
`MALICIOUS_PROCESS`	Menunjukkan proses yang diduga berbahaya berdasarkan kecerdasan ancaman atau analisis perilaku. Misalnya, ini termasuk malware yang dikenal, pintu belakang, atau alat tidak sah yang dijalankan dalam lingkungan instance atau kontainer.

Nama indikator	Deskripsi
MISCONFIGURATION	Menunjukkan bahwa sumber daya yang terlibat dalam urutan serangan memiliki kesalahan konfigurasi keamanan yang dapat meningkatkan dampak potensial. Contohnya termasuk kebijakan akses administratif, pembuatan versi yang dinonaktifkan, atau enkripsi yang hilang. Kesalahan konfigurasi ini diidentifikasi oleh. AWS Security Hub CSPM Untuk informasi selengkapnya, lihat Jenis sifat yang didukung di Panduan AWS Security Hub CSPM Pengguna.
REACHABILITY	Menunjukkan bahwa sumber daya yang terlibat dalam urutan serangan dapat dijangkau dari internet atau dapat diakses publik. Contohnya termasuk instans Amazon EC2 yang dapat dijangkau internet, kluster Amazon EKS, kluster Amazon ECS, atau bucket Amazon S3 yang dapat diakses publik. Untuk informasi selengkapnya, lihat Jenis sifat yang didukung di Panduan AWS Security Hub CSPM Pengguna.
SENSITIVE_DATA	Menunjukkan bahwa bucket Amazon S3 yang terlibat dalam urutan serangan berisi data sensitif, seperti yang diidentifikasi oleh Amazon Macie. AWS Security Hub CSPM
SUSPICIOUS_NETWORK	Jaringan ini dikaitkan dengan skor reputasi rendah yang diketahui, seperti penyedia jaringan pribadi virtual (VPN) berisiko dan layanan proxy.
SUSPICIOUS_PROCESS	Menunjukkan proses mencurigakan yang diidentifikasi sebagai anomali berdasarkan kecerdasan ancaman atau analisis perilaku. Misalnya, ini termasuk pola eksekusi proses yang tidak biasa, hubungan orangtua-anak yang tidak terduga, atau proses dengan karakteristik mencurigakan dalam sebuah instance, atau lingkungan kontainer.
SUSPICIOUS_USER_AGENT	Agen pengguna dikaitkan dengan aplikasi mencurigakan atau dieksploitasi yang berpotensi diketahui, seperti klien Amazon S3 dan alat serangan.
TOR_IP	Alamat IP dikaitkan dengan node keluar Tor.

Nama indikator	Deskripsi
`UNUSUAL_API_FOR_ACCOUNT`	Menunjukkan bahwa AWS API dipanggil secara anomali, berdasarkan garis dasar historis akun. Untuk informasi selengkapnya, lihat Perilaku anomali.
`UNUSUAL_ASN_FOR_ACCOUNT`	Menunjukkan bahwa Nomor Sistem Otonom (ASN) diidentifikasi sebagai anomali, berdasarkan dasar historis akun tersebut. Untuk informasi selengkapnya, lihat Perilaku anomali.
`UNUSUAL_ASN_FOR_USER`	Menunjukkan bahwa Nomor Sistem Otonom (ASN) diidentifikasi sebagai anomali, berdasarkan garis dasar historis pengguna. Untuk informasi selengkapnya, lihat Perilaku anomali.
`VULNERABILITY`	Menunjukkan bahwa sumber daya yang terlibat dalam urutan serangan telah diketahui kerentanan dengan tingkat keparahan kritis, tinggi, sedang, atau rendah. Nilai indikator termasuk pengidentifikasi CVE dan tingkat keparahannya. Kerentanan ini terdeteksi oleh Amazon Inspector dan dapat meningkatkan dampak potensial dari urutan serangan. Untuk informasi selengkapnya tentang tingkat keparahan, lihat Memahami tingkat keparahan di Panduan Pengguna Amazon Inspector.

Taktik MITRE

Bidang ini menentukan taktik MITRE ATT&CK yang dicoba oleh aktor ancaman melalui urutan serangan. GuardDuty menggunakan kerangka kerja MITRE ATT&ACK yang menambahkan konteks ke seluruh urutan serangan. Warna yang digunakan GuardDuty konsol untuk menentukan tujuan ancaman yang telah digunakan oleh aktor ancaman, sejajar dengan warna yang menunjukkan kritis, tinggi, sedang, dan rendahTingkat keparahan temuan.

Indikator jaringan

Indikator mencakup kombinasi nilai indikator jaringan yang menjelaskan mengapa jaringan menunjukkan perilaku yang mencurigakan. Bagian ini hanya berlaku jika Indikator menyertakan `SUSPICIOUS_NETWORK` atau`MALICIOUS_IP`. Contoh berikut menunjukkan bagaimana indikator jaringan dapat dikaitkan dengan indikator, di mana:

- *AnyCompany*adalah Sistem Otonom (AS).

- `TUNNEL_VPN`,`IS_ANONYMOUS`, dan `ALLOWS_FREE_ACCESS` merupakan indikator jaringan.

```
...{
    "key": "SUSPICIOUS_NETWORK",
    "values": [{
        "AnyCompany": [
            "TUNNEL_VPN",
            "IS_ANONYMOUS",
            "ALLOWS_FREE_ACCESS"
        ]
    }]
}
...
```

Tabel berikut mencakup nilai indikator jaringan dan deskripsinya. Tag ini ditambahkan berdasarkan data intelijen ancaman yang GuardDuty dikumpulkan dari sumber seperti Spur

Nilai indikator jaringan	Deskripsi
`TUNNEL_VPN`	Jaringan atau alamat IP dikaitkan dengan jenis terowongan VPN. Ini mengacu pada protokol khusus yang membantu membangun koneksi terenkripsi yang aman antara dua titik melalui jaringan publik.
`TUNNEL_PROXY`	Jaringan atau alamat IP dikaitkan dengan jenis terowongan Proxy. Ini mengacu pada protokol khusus yang membantu membangun koneksi melalui server proxy.
`TUNNEL_RDP`	Jaringan atau alamat IP dikaitkan dengan menggunakan metode enkapsulasi lalu lintas desktop jarak jauh (RDP) dalam protokol lain untuk meningkatkan keamanan, melewati pembatasan jaringan, atau mengaktifkan akses jarak jauh melalui firewall.
`IS_ANONYMOUS`	Jaringan atau alamat IP dikaitkan dengan layanan anonim atau proxy yang dikenal. Ini mungkin menunjukkan potensi aktivitas mencuriga kan yang bersembunyi di balik jaringan anonim.
`KNOWN_THR EAT_OPERATOR`	Jaringan atau alamat IP dikaitkan dengan penyedia terowongan berisiko yang diketahui. Ini menunjukkan bahwa aktivitas mencuriga

Nilai indikator jaringan	Deskripsi
	kan telah terdeteksi dari alamat IP yang ditautkan ke VPN, proxy, atau layanan tunneling lainnya yang sering digunakan untuk tujuan jahat.
ALLOWS_FREE_ACCESS	Jaringan atau alamat IP dikaitkan dengan operator terowongan yang memungkinkan akses ke layanannya tanpa memerlukan otentikasi atau pembayaran. Ini mungkin juga termasuk akun percobaan atau pengalaman penggunaan terbatas yang ditawarkan oleh berbagai layanan online.
ALLOWS_CRYPTO	Jaringan atau alamat IP dikaitkan dengan penyedia terowongan (seperti VPN atau layanan proxy) yang secara eksklusif menerima cryptocurrency atau mata uang digital lainnya sebagai metode pembayaran.
ALLOWS_TORRENTS	Jaringan atau alamat IP dikaitkan dengan layanan atau platform yang memungkinkan lalu lintas torrent. Layanan semacam itu sering dikaitkan dengan mendukung dan menggunakan torrent, dan kegiatan pengelakan hak cipta.
RISK_CALLBACK_PROXY	Jaringan atau alamat IP dikaitkan dengan perangkat yang dikenal untuk mengarahkan lalu lintas untuk proxy perumahan, proxy malware, atau jaringan tipe proxy callback lainnya. Ini tidak berarti semua aktivitas di jaringan terkait dengan proxy, melainkan bahwa jaringan memiliki kemampuan untuk merutekan lalu lintas atas nama jaringan proxy ini.
RISK_GEO_MISMATCH	Indikator ini menunjukkan bahwa pusat data atau lokasi hosting jaringan berbeda dari lokasi yang diharapkan dari pengguna dan perangkat di belakangnya. Jika nilai indikator ini tidak ada, itu tidak berarti bahwa tidak ada ketidakcocokan. Ini mungkin menyiratkan bahwa tidak ada cukup data untuk mengkonfirmasi perbedaan tersebut.
IS_SCANNER	Jaringan atau alamat IP dikaitkan dengan melakukan upaya login persisten terhadap formulir web.

Nilai indikator jaringan	Deskripsi
`RISK_WEB_SCRAPING`	Jaringan alamat IP dikaitkan dengan klien web otomatis dan aktivitas web terprogram lainnya.
`CLIENT_BEHAVIOR_FILE_SHARING`	Jaringan atau alamat IP dikaitkan dengan perilaku klien yang menunjukkan aktivitas berbagi file, seperti jaringan peer-to-peer (P2P), atau protokol berbagi file.
`CATEGORY_COMMERCIAL_VPN`	Jaringan atau alamat IP dikaitkan dengan operator terowongan yang dikategorikan sebagai layanan Commercial Virtual Private Network (VPN) tradisional yang beroperasi dalam ruang pusat data.
`CATEGORY_FREE_VPN`	Jaringan atau alamat IP dikaitkan dengan operator terowongan yang dikategorikan sebagai layanan VPN gratis.
`CATEGORY_RESIDENTIAL_PROXY`	Alamat jaringan atau IP dikaitkan dengan operator terowongan yang dikategorikan sebagai SDK, malware, atau layanan proxy bersumber.
`OPERATOR_XXX`	Nama penyedia layanan yang mengoperasikan terowongan ini.

Aturan Deteksi Kustom menemukan detail

Detail dalam temuan Aturan Deteksi Kustom bergantung pada sumber data aturan yang menghasilkannya.

Temuan dari AWS CloudTrail aturan

Temuan dari AWS CloudTrail aturan menggunakan `Service.Detection.Sequence` struktur yang sama seperti[Detail pencarian urutan serangan](). Bidang Aktor, Titik Akhir, Sumber Daya, dan Sinyal berbagi skema yang sama. Detail berikut khusus untuk Aturan Deteksi Kustom.

Jenis

Jenis temuan mengikuti format`Tactic:Service/Technique`. Misalnya, `Persistence:EC2/ExternalRemoteServices`.

Sinyal

Setiap sinyal mewakili satu peristiwa aturan yang cocok. `Name`Bidang berisi nama Aturan Deteksi Kustom, dan `SignalIndicators` berisi taktik dan teknik MITRE ATT&CK®. Beberapa sinyal dengan aturan yang sama dapat muncul ketika aturan cocok dengan beberapa peristiwa dalam jendela agregasi.

Aktor

Rincian tentang prinsip-prinsip IAM yang melakukan aktivitas yang terdeteksi. Termasuk jenis pengguna (seperti `AssumedRole` atau`IAMUser`), informasi kredensi, dan detail sesi termasuk peran penerbitan ARN dan status MFA.

Sumber Daya

Detail tentang AWS sumber daya yang terlibat dalam aktivitas yang terdeteksi, jika berlaku, seperti instans Amazon EC2, bucket Amazon S3, atau kunci akses IAM.

Titik akhir

Detail tentang titik akhir jaringan dari mana aktivitas berasal. Termasuk alamat IP, lokasi geografis (kota dan negara), dan nama dan nomor sistem otonom (AS).

Temuan dari aturan Runtime Monitoring

Temuan dari aturan Runtime Monitoring menggunakan struktur yang sama dengan temuan Runtime Monitoring lainnya, termasuk detail runtime dari proses yang terlibat. Untuk informasi selengkapnya, lihat Detail temuan Pemantauan Runtime. Detail berikut khusus untuk Aturan Deteksi Kustom:

Jenis

Jenis temuan mengikuti format`Tactic:Runtime/Technique`. Misalnya, `Persistence:Runtime/SuspiciousCommand`.

Aturan

`CustomDetectionRuleName`Bidang berisi nama Aturan Deteksi Kustom yang menghasilkan temuan.

Konteks

`Service.RuntimeDetails.Context`Bidang menggambarkan aktivitas yang cocok. Bidang yang termasuk dalam temuan bergantung pada aturan:

- Aturan yang menghasilkan `SensitiveFileRead` dan `SensitiveFileModified` temuan termasuk `FilePath` dan`FileOperation`.
- Sebagian besar aturan yang menghasilkan `SuspiciousCommand` temuan termasuk`CommandLineExample`, dan beberapa juga termasuk`ServiceName`. Aturan yang mendeteksi aktivitas pada file tertentu, seperti mengubah izin file, termasuk sebagai `FilePath` gantinya, dan `FileOperation` kapan itu berlaku.
- Aturan yang menghasilkan `SuspiciousTool` temuan termasuk `ToolName` dan`ToolCategory`.

Sumber Daya

Setiap temuan mencakup sumber daya tunggal, seperti instance, tugas, atau wadah. Untuk informasi selengkapnya tentang bagaimana GuardDuty grup memberi sinyal, lihatMenemukan agregasi.

Rincian pengguna database RDS (DB)

> **Note**
>
> Bagian ini berlaku untuk temuan saat Anda mengaktifkan fitur Perlindungan RDS di GuardDuty. Untuk informasi selengkapnya, lihat GuardDuty Perlindungan RDS.

GuardDuty Temuan ini memberikan rincian pengguna dan otentikasi berikut dari database yang berpotensi dikompromikan:

- Pengguna — Nama pengguna yang digunakan untuk melakukan upaya login anomali.
- Aplikasi — Nama aplikasi yang digunakan untuk melakukan upaya login anomali.
- Database — Nama instance database yang terlibat dalam upaya login anomali.
- SSL — Versi Secure Socket Layer (SSL) yang digunakan untuk jaringan.
- Metode autentikasi — Metode otentikasi yang digunakan oleh pengguna yang terlibat dalam temuan.

Untuk informasi tentang sumber daya yang berpotensi dikompromikan, lihatSumber daya.

Detail temuan Pemantauan Runtime

> **Note**
>
> Detail ini mungkin tersedia hanya jika GuardDuty menghasilkan salah satuGuardDuty Jenis penemuan Runtime Monitoring.

Bagian ini berisi rincian runtime seperti detail proses dan konteks yang diperlukan. Detail proses menjelaskan informasi tentang proses yang diamati, dan konteks runtime menjelaskan informasi tambahan tentang aktivitas yang berpotensi mencurigakan.

Detail proses

- Nama — Nama proses.
- Jalur yang dapat dieksekusi — Jalur absolut dari file yang dapat dieksekusi proses.
- Executable SHA-256 — SHA256 Hash dari proses yang dapat dieksekusi.
- Namespace PID — ID proses dalam namespace PID sekunder selain namespace PID tingkat host. Untuk proses di dalam wadah, itu adalah ID proses yang diamati di dalam wadah.
- Direktori kerja saat ini — Direktori kerja saat ini dari proses.
- ID Proses — ID yang ditetapkan untuk proses oleh sistem operasi.
- StartTime — Waktu ketika proses dimulai. Ini dalam format string tanggal UTC (`2023-03-22T19:37:20.168Z`).
- UUID — ID unik yang ditetapkan untuk proses oleh. GuardDuty
- UUID Induk — ID unik dari proses induk. ID ini ditetapkan ke proses induk oleh GuardDuty.
- Pengguna — Pengguna yang menjalankan proses.
- User ID — ID pengguna yang menjalankan proses.
- ID pengguna yang efektif — ID pengguna yang efektif dari proses pada saat acara berlangsung.
- Silsilah — Informasi tentang nenek moyang proses.
  - ID Proses — ID yang ditetapkan untuk proses oleh sistem operasi.
  - UUID — ID unik yang ditetapkan untuk proses oleh. GuardDuty
  - Jalur yang dapat dieksekusi — Jalur absolut dari file yang dapat dieksekusi proses.
  - ID pengguna yang efektif — ID pengguna yang efektif dari proses pada saat acara berlangsung.

- UUID Induk — ID unik dari proses induk. ID ini ditetapkan ke proses induk oleh GuardDuty.
- Waktu Mulai — Waktu ketika proses dimulai.
- Namespace PID — ID proses dalam namespace PID sekunder selain namespace PID tingkat host. Untuk proses di dalam wadah, itu adalah ID proses yang diamati di dalam wadah.
- User ID — User ID pengguna yang menjalankan proses.
- Nama — Nama proses.

Konteks runtime

Dari bidang berikut, temuan yang dihasilkan mungkin hanya mencakup bidang-bidang yang relevan dengan jenis temuan.

- Mount Source - Jalur pada host yang dipasang oleh wadah.
- Mount Target - Jalur dalam wadah yang dipetakan ke direktori host.
- Jenis Sistem File - Merupakan jenis sistem file yang dipasang.
- Bendera - Merupakan opsi yang mengontrol perilaku acara yang terlibat dalam temuan ini.
- Memodifikasi Proses — Informasi tentang proses yang membuat atau memodifikasi biner, skrip, atau pustaka, di dalam wadah saat runtime.
- Modified At — Stempel waktu di mana proses membuat atau memodifikasi biner, skrip, atau pustaka di dalam wadah saat runtime. Bidang ini dalam format string tanggal UTC (`2023-03-22T19:37:20.168Z`).
- Library Path — Jalur ke perpustakaan baru yang dimuat.
- LD Preload Value — Nilai variabel `LD_PRELOAD` lingkungan.
- Socket Path — Jalur ke soket Docker yang diakses.
- Runc Binary Path — Jalan menuju `runc` biner.
- Release Agent Path - Jalur ke file agen `cgroup` rilis.
- Contoh Baris Perintah — Contoh baris perintah yang terlibat dalam aktivitas yang berpotensi mencurigakan.
- Kategori Alat - Kategori yang dimiliki alat tersebut. Beberapa contohnya adalah Backdoor Tool, Pentest Tool, Network Scanner, dan Network Sniffer.
- Nama Alat — Nama alat yang berpotensi mencurigakan.
- Operasi File — Jenis operasi file yang memicu temuan, seperti Write, Delete, Rename, Link, atau Symlink.

- File Path — Path dari file sensitif yang telah dimodifikasi. Modifikasi termasuk menulis, menghapus, mengganti nama, tautan, atau operasi symlink.
- Jalur File Terkait — Semua jalur file dimodifikasi oleh proses yang sama yang memicu temuan, hingga maksimum 25 jalur.
- Script Path — Jalur ke skrip yang dieksekusi yang menghasilkan temuan.
- Threat File Path — Jalur mencurigakan di mana rincian intelijen ancaman ditemukan.
- Nama Layanan — Nama layanan keamanan yang telah dinonaktifkan.
- Nama Modul — Nama modul yang dimuat ke dalam kernel.
- Modul SHA256 — Hash SHA256 modul.
- Module File Path — Path ke modul dimuat ke kernel.

Detail pemindaian volume EBS

> **Note**
>
> Bagian ini berlaku untuk temuan saat Anda mengaktifkan pemindaian GuardDuty-initiated malwarePerlindungan Malware untuk EC2.

Pemindaian volume EBS memberikan detail tentang volume EBS yang melekat pada instans EC2 atau beban kerja kontainer yang berpotensi dikompromikan.

- Scan ID — Pengidentifikasi pemindaian malware.
- Pemindaian dimulai pada — Tanggal dan waktu ketika pemindaian malware dimulai.
- Pemindaian selesai pada — Tanggal dan waktu pemindaian malware selesai.
- Trigger Finding ID — ID temuan dari GuardDuty temuan yang memulai pemindaian malware ini.
- Sumber — Nilai potensial adalah `Bitdefender` dan`Amazon`.

  Untuk informasi selengkapnya tentang mesin pemindai yang digunakan untuk mendeteksi malware, lihatGuardDuty mesin pemindai deteksi malware.
- Deteksi pemindaian — Tampilan lengkap detail dan hasil untuk setiap pemindaian malware.
  - Jumlah item yang dipindai - Jumlah total file yang dipindai. Ini memberikan rincian sepertitotalGb,`files`, dan`volumes`.

- Jumlah item yang terdeteksi ancaman — Jumlah total berbahaya yang `files` terdeteksi selama pemindaian.
- Detail ancaman tingkat keparahan tertinggi — Rincian ancaman tingkat keparahan tertinggi yang terdeteksi selama pemindaian dan jumlah file berbahaya. Ini memberikan rincian seperti`severity`,`threatName`, dan`count`.
- Ancaman terdeteksi oleh Nama - Elemen kontainer mengelompokkan ancaman dari semua tingkat keparahan. Ini memberikan rincian seperti`itemCount`,`uniqueThreatNameCount`,`shortened`, dan`threatNames`.

Perlindungan Malware untuk detail pencarian EC2

> **Note**
>
> Bagian ini berlaku untuk temuan saat Anda mengaktifkan pemindaian GuardDuty-initiated malwarePerlindungan Malware untuk EC2.

Saat Perlindungan Malware untuk pemindaian EC2 mendeteksi malware, Anda dapat melihat detail pemindaian dengan memilih temuan yang sesuai di halaman Temuan di https://console.aws.amazon.com/guardduty/konsol. Tingkat keparahan Perlindungan Malware Anda untuk temuan EC2 tergantung pada tingkat keparahan GuardDuty temuan.

Informasi berikut tersedia di bawah bagian Ancaman terdeteksi di panel detail.

- Nama — Nama ancaman, diperoleh dengan mengelompokkan file dengan deteksi.
- Keparahan — Tingkat keparahan ancaman yang terdeteksi.
- Hash — File. SHA-256
- Jalur file — Lokasi file berbahaya dalam volume EBS.
- Nama file — Nama file di mana ancaman terdeteksi.
- Volume ARN — ARN dari volume EBS yang dipindai.

Informasi berikut tersedia di bawah bagian Detail pemindaian Malware di panel detail.

- Scan ID — ID pemindaian dari pemindaian malware.
- Pemindaian dimulai pada — Tanggal dan waktu pemindaian dimulai.

- Pemindaian selesai pada — Tanggal dan waktu pemindaian selesai.
- File yang dipindai — Jumlah total file dan direktori yang dipindai.
- Total GB yang dipindai — Jumlah penyimpanan yang dipindai selama proses berlangsung.
- Trigger finding ID — ID temuan dari GuardDuty temuan yang memulai pemindaian malware ini.
- Informasi berikut tersedia di bawah bagian Detail volume di panel detail.
  - Volume ARN — Nama Sumber Daya Amazon (ARN) dari volume.
  - Snapshotarn — ARN dari snapshot volume EBS.
  - Status — Status pemindaian volume, sepertiRunning,Skipped, danCompleted.
  - Jenis enkripsi — Jenis enkripsi yang digunakan untuk mengenkripsi volume. Misalnya, CMCMK.
  - Nama perangkat — Nama perangkat. Misalnya, /dev/xvda.

Detail temuan Perlindungan Malware untuk S3

Detail pemindaian malware berikut tersedia saat Anda mengaktifkan keduanya GuardDuty dan Perlindungan Malware untuk S3 di: Akun AWS

- Ancaman — Daftar ancaman yang terdeteksi selama pemindaian malware.

> **Beberapa potensi ancaman dalam file arsip**
>
> Jika Anda memiliki file arsip dengan potensi beberapa ancaman di dalamnya, Perlindungan Malware untuk S3 hanya melaporkan ancaman pertama yang terdeteksi. Setelah ini, status pemindaian ditandai sebagai selesai. GuardDuty menghasilkan jenis temuan terkait dan juga mengirimkan EventBridge peristiwa yang dihasilkannya. Untuk informasi selengkapnya tentang memantau pemindaian objek Amazon S3 menggunakan EventBridge peristiwa, lihat skema pemberitahuan contoh untuk THREATS_FOUND di. Hasil pemindaian objek S3

- Jalur item - Daftar jalur item bersarang dan detail hash dari objek S3 yang dipindai.
  - Jalur item bersarang - Jalur item dari objek S3 yang dipindai tempat ancaman terdeteksi.

    Nilai bidang ini hanya tersedia jika objek tingkat atas adalah arsip dan jika ancaman terdeteksi di dalam arsip.
  - Hash — Hash dari ancaman yang terdeteksi dalam temuan ini.

> **Note**
>
> Dalam kasus di mana hash tidak dapat dihitung, hasil pemindaian masih dikirimkan dan nilai hash default ke string kosong (). SHA-256 `e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`

- Sumber — Nilai potensial adalah `Bitdefender` dan`Amazon`.

  Untuk informasi selengkapnya tentang mesin pemindai yang digunakan untuk mendeteksi malware, lihatGuardDuty mesin pemindai deteksi malware.

Tindakan

Tindakan temuan memberikan rincian tentang jenis aktivitas yang memicu temuan. Informasi yang tersedia bervariasi berdasarkan tipe tindakan.

Tipe tindakan – Tipe aktivitas temuan. Nilai ini dapat berupa NETWORK_CONNECTION, PORT_PROBE, DNS_REQUEST,, atau RDS_LOGIN_ATTACT. AWS_API_CALL Informasi yang tersedia bervariasi berdasarkan tipe tindakan:

- NETWORK_CONNECTION - Menunjukkan bahwa lalu lintas jaringan dipertukarkan antara instans EC2 yang diidentifikasi dan host jarak jauh. Tipe tindakan ini memiliki informasi tambahan berikut:
  - Arah koneksi — Arah koneksi jaringan diamati dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan. Nilai bisa jadi salah satu dari nilai berikut:
    - INBOUND - Menunjukkan bahwa host jarak jauh memulai koneksi ke port lokal pada instans EC2 yang diidentifikasi di akun Anda.
    - OUTBOUND - Menunjukkan bahwa instans EC2 yang diidentifikasi memulai koneksi ke host jarak jauh.
    - TIDAK DIKETAHUI — Menunjukkan bahwa tidak GuardDuty dapat menentukan arah koneksi.
  - Protokol — Protokol koneksi jaringan diamati dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
  - IP lokal — Alamat IP sumber asli dari lalu lintas yang memicu temuan. Info ini dapat digunakan untuk membedakan antara alamat IP dari lapisan perantara yang dilalui arus lalu lintas, dan alamat IP sumber asal dari lalu lintas yang memicu temuan. Misalnya, alamat IP pod EKS berbeda dengan alamat IP instans tempat pod EKS berjalan.

  - Diblokir – Menunjukkan apakah port yang ditargetkan diblokir.
- PORT_PROBE - Menunjukkan bahwa host jarak jauh memeriksa instans EC2 yang diidentifikasi pada beberapa port terbuka. Tipe tindakan ini memiliki informasi tambahan berikut:
  - IP lokal — Alamat IP sumber asli dari lalu lintas yang memicu temuan. Info ini dapat digunakan untuk membedakan antara alamat IP dari lapisan perantara yang dilalui arus lalu lintas, dan alamat IP sumber asal dari lalu lintas yang memicu temuan. Misalnya, alamat IP pod EKS berbeda dengan alamat IP instans tempat pod EKS berjalan.
  - Diblokir – Menunjukkan apakah port yang ditargetkan diblokir.
- DNS_REQUEST - Menunjukkan bahwa instans EC2 yang diidentifikasi menanyakan nama domain. Tipe tindakan ini memiliki informasi tambahan berikut:
  - Protokol — Protokol koneksi jaringan diamati dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
  - Diblokir – Menunjukkan apakah port yang ditargetkan diblokir.
- AWS_API_CALL— Menunjukkan bahwa AWS API dipanggil. Tipe tindakan ini memiliki informasi tambahan berikut:
  - API — Nama operasi API yang dipanggil dan dengan demikian diminta GuardDuty untuk menghasilkan temuan ini.

    > **Note**
    >
    > Operasi ini juga dapat mencakup peristiwa non-API yang ditangkap oleh AWS CloudTrail. Untuk informasi selengkapnya, lihat Non-API peristiwa yang ditangkap oleh CloudTrail.

  - User Agent — Agen pengguna yang membuat permintaan API. Nilai ini memberi tahu Anda apakah panggilan dilakukan dari Konsol Manajemen AWS, AWS layanan, AWS SDK, atau. AWS CLI
  - KODE KESALAHAN - Jika temuan dipicu oleh panggilan API yang gagal, ini menampilkan kode kesalahan untuk panggilan itu.
  - Nama layanan — Nama DNS dari layanan yang mencoba membuat panggilan API yang memicu temuan.
- RDS_LOGIN_ATTACT - Menunjukkan bahwa upaya login dilakukan ke database yang berpotensi dikompromikan dari alamat IP jarak jauh.

- Alamat IP — Alamat IP jarak jauh yang digunakan untuk melakukan upaya login yang berpotensi mencurigakan.

Aktor atau Target

Temuan memiliki bagian Aktor jika peran Sumber Daya adalah `TARGET`. Ini menunjukkan bahwa sumber daya Anda ditargetkan oleh aktivitas mencurigakan, dan bagian Aktor berisi detail tentang entitas yang menargetkan sumber daya Anda.

Temuan memiliki bagian Target jika peran Sumber Daya adalah `ACTOR`. Hal ini menunjukkan bahwa sumber daya Anda terlibat dalam aktivitas yang mencurigakan terhadap host jarak jauh, dan bagian ini berisi informasi tentang IP atau domain yang ditargetkan sumber daya Anda.

Informasi yang tersedia di bagian Aktor atau Target dapat mencakup hal-hal berikut:

- Afiliasi — Detail tentang apakah AWS akun pemanggil API jarak jauh terkait dengan lingkungan Anda GuardDuty . Jika nilai ini`true`, pemanggil API berafiliasi dengan akun Anda dalam beberapa cara; jika`false`, pemanggil API berasal dari luar lingkungan Anda.
- ID Akun Jarak Jauh — ID akun yang memiliki alamat IP keluar yang digunakan untuk mengakses sumber daya di jaringan akhir.
- Alamat IP — Alamat IP yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Lokasi — Informasi lokasi untuk alamat IP yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- Organisasi — informasi organisasi ISP dari alamat IP yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Port — Nomor port yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Domain — Domain yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Domain dengan akhiran — Domain tingkat kedua dan teratas yang terlibat dalam aktivitas yang berpotensi mendorong GuardDuty untuk menghasilkan temuan. Untuk daftar domain tingkat atas dan tingkat kedua, lihat daftar akhiran publik.

Detail geolokasi

GuardDuty menentukan lokasi dan jaringan permintaan dengan menggunakan database MaxMind GeoIP. MaxMind melaporkan akurasi data mereka yang sangat tinggi di tingkat negara, meskipun akurasi bervariasi sesuai dengan faktor-faktor seperti negara dan jenis alamat IP.

Untuk informasi selengkapnya MaxMind, lihat Geolokasi MaxMind IP. Jika Anda yakin salah satu data GeoIP salah, kirimkan permintaan koreksi ke Data MaxMind GeoIP2 MaxMind yang Benar.

Informasi tambahan

Semua temuan memiliki bagian Informasi tambahan yang dapat mencakup informasi berikut:

- Nama daftar ancaman — Nama daftar ancaman yang mencakup alamat IP atau nama domain yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- Sampel — Nilai benar atau salah yang menunjukkan apakah ini adalah temuan sampel.
- Diarsipkan — Nilai benar atau salah yang menunjukkan apakah temuan ini telah diarsipkan.
- Tidak biasa — Detail aktivitas yang tidak diamati secara historis. Ini dapat mencakup pengguna yang tidak biasa (sebelumnya tidak diamati), lokasi, waktu, bucket, perilaku login, atau ASN Org.
- Protokol yang tidak biasa — Protokol koneksi jaringan yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Detail agen — Detail tentang agen keamanan yang saat ini digunakan di klaster EKS di Anda Akun AWS. Ini hanya berlaku untuk jenis pencarian Pemantauan Runtime EKS.
  - Versi agen — Versi agen GuardDuty keamanan.
  - Agen Id — Identifier unik dari agen GuardDuty keamanan.

Bukti

Temuan berdasarkan intelijen ancaman memiliki bagian Bukti yang mencakup informasi berikut:

- Detail intelijen ancaman — Nama daftar ancaman tempat yang dikenali `Threat name` muncul.
- Nama ancaman — Nama keluarga malware atau pengenal lain yang terkait dengan ancaman.
- File ancaman SHA256 — SHA256 dari file yang menghasilkan temuan.

Perilaku anomali

Jenis temuan yang berakhir AnomalousBehaviormenunjukkan bahwa temuan tersebut dihasilkan oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua permintaan API ke akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan taktik yang digunakan oleh musuh. Model ML melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi tempat permintaan dibuat, dan API khusus yang diminta.

Detail tentang faktor permintaan API yang tidak biasa untuk identitas CloudTrail pengguna yang memanggil permintaan dapat ditemukan di detail temuan. Identitas didefinisikan oleh Elemen CloudTrail UserIdentity, dan nilai yang mungkin adalah`Root`:`IAMUser`,,,, `AssumedRole` `FederatedUser`AWSAccount, atau. `AWSService`

Selain detail yang tersedia untuk semua GuardDuty temuan yang terkait dengan aktivitas API, AnomalousBehaviortemuan memiliki detail tambahan yang diuraikan di bagian berikut. Detail ini dapat dilihat di konsol dan juga tersedia di JSON temuan.

- Anomalous API — Daftar permintaan API yang dipanggil oleh identitas pengguna di dekat permintaan API utama yang terkait dengan temuan tersebut. Panel ini selanjutnya memecah detail peristiwa API dengan cara berikut.
  - API pertama yang terdaftar adalah API utama, yang merupakan permintaan API yang terkait dengan aktivitas berisiko tertinggi yang diamati. Ini adalah API yang memicu temuan dan berkorelasi dengan tahap serangan dari tipe temuan. Ini juga merupakan API yang diuraikan di bagian Tindakan di konsol, dan di JSON temuan.
  - API lain yang terdaftar adalah API anomali tambahan dari identitas pengguna terdaftar yang diamati di sekitar API utama. Jika hanya ada satu API pada daftar, model ML tidak mengidentifikasi permintaan API tambahan dari identitas pengguna sebagai anomali.
  - Daftar API dibagi berdasarkan apakah API berhasil dipanggil, atau jika API tidak berhasil dipanggil, yang berarti respons kesalahan diterima. Jenis respons kesalahan yang diterima tercantum di atas setiap API yang tidak berhasil disebut. Jenis respons kesalahan yang mungkin adalah:`access denied`,`access denied exception`,`auth failure`,`instance limit exceeded`,`invalid permission - duplicate`,`invalid permission - not found`, dan`operation not permitted`.
  - API dikategorikan oleh layanan yang terkait.
  - Untuk konteks lebih lanjut, pilih API Historis untuk melihat detail tentang API teratas, hingga maksimum 20, biasanya terlihat untuk identitas pengguna dan semua pengguna dalam akun. API ditandai Langka (kurang dari sebulan sekali), Jarang (beberapa kali sebulan), atau Sering

(harian hingga mingguan), tergantung pada seberapa sering mereka digunakan dalam akun Anda.

- Perilaku Tidak Biasa (Akun) — Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk akun Anda.

> **Perilaku yang diprofilkan**
>
> GuardDuty terus belajar tentang aktivitas dalam akun Anda berdasarkan peristiwa yang disampaikan. Kegiatan ini dan frekuensi yang diamati dikenal sebagai perilaku yang diprofilkan.

Informasi yang dilacak di panel ini mencakup:

- ASN Org — Org Autonomous System Number (ASN) tempat panggilan API anomali dibuat.
- Nama Pengguna – Nama pengguna yang membuat panggilan API anomali.
- User Agent — Agen pengguna yang digunakan untuk membuat panggilan API anomali. Agen pengguna adalah metode yang digunakan untuk membuat panggilan seperti `aws-cli` atau `Botocore`.
- Tipe Pengguna – Tipe pengguna yang membuat panggilan API anomali. Kemungkinan nilainya adalah `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER`, atau `ROLE`.
- Bucket — Nama bucket S3 yang sedang diakses.

- Perilaku Tidak Biasa (Identitas Pengguna) - Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk Identitas Pengguna yang terlibat dengan temuan tersebut. Ketika perilaku tidak diidentifikasi sebagai historis, ini berarti model GuardDuty ML sebelumnya tidak melihat identitas pengguna ini membuat panggilan API ini dengan cara ini dalam periode pelatihan. Berikut adalah detail tambahan tentang Identitas Pengguna yang tersedia:
  - ASN Org – ASN Org tempat panggilan API anomali dibuat.
  - User Agent — Agen pengguna yang digunakan untuk membuat panggilan API anomali. Agen pengguna adalah metode yang digunakan untuk membuat panggilan seperti `aws-cli` atau `Botocore`.
  - Bucket — Nama bucket S3 yang sedang diakses.
- Perilaku Tidak Biasa (Bucket) — Bagian ini memberikan detail tambahan tentang perilaku yang diprofilkan untuk bucket S3 yang terkait dengan temuan tersebut. Jika perilaku tidak diidentifikasi sebagai historis, ini berarti model GuardDuty ML sebelumnya tidak pernah melihat panggilan API

yang dilakukan ke bucket ini dengan cara ini dalam periode pelatihan. Informasi yang dilacak di bagian ini meliputi:

- ASN Org – ASN Org tempat panggilan API anomali dibuat.
- Nama Pengguna – Nama pengguna yang membuat panggilan API anomali.
- User Agent — Agen pengguna yang digunakan untuk membuat panggilan API anomali. Agen pengguna adalah metode yang digunakan untuk membuat panggilan seperti `aws-cli` atau `Botocore`.
- Tipe Pengguna – Tipe pengguna yang membuat panggilan API anomali. Kemungkinan nilainya adalah `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER`, atau `ROLE`.

> **Note**
>
> Untuk konteks lebih lanjut tentang perilaku historis, pilih Perilaku historis di bagian Perilaku Tidak Biasa (Akun), ID Pengguna, atau Bucket untuk melihat detail tentang perilaku yang diharapkan di akun Anda untuk masing-masing kategori berikut: Langka (kurang dari sebulan sekali), Jarang (beberapa kali sebulan), atau Sering (harian hingga mingguan), tergantung seberapa sering mereka digunakan dalam akun Anda.

- Perilaku Tidak Biasa (Database) - Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk instance database yang terkait dengan temuan. Ketika perilaku tidak diidentifikasi sebagai historis, itu berarti bahwa model GuardDuty ML sebelumnya tidak melihat upaya login yang dilakukan ke instance database ini dengan cara ini dalam periode pelatihan. Informasi yang dilacak untuk bagian ini di panel temuan meliputi:
  - Nama pengguna — Nama pengguna yang digunakan untuk melakukan upaya login anomali.
  - ASN Org — Org ASN tempat upaya login anomali dilakukan.
  - Nama aplikasi — Nama aplikasi yang digunakan untuk melakukan upaya login anomali.
  - Nama database — Nama instance database yang terlibat dalam upaya login anomali.

  Bagian perilaku historis memberikan lebih banyak konteks tentang nama Pengguna yang diamati sebelumnya, Org ASN, nama Aplikasi, dan nama Database untuk database terkait. Setiap nilai unik memiliki hitungan terkait yang mewakili berapa kali nilai ini diamati dalam peristiwa login yang berhasil.
- Perilaku yang tidak biasa (klaster Akun Kubernetes, namespace Kubernetes, dan nama pengguna Kubernetes) — Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk klaster Kubernetes dan namespace yang terkait dengan temuan tersebut. Ketika perilaku tidak

diidentifikasi sebagai historis, itu berarti bahwa model GuardDuty ML sebelumnya tidak mengamati akun, klaster, namespace, atau nama pengguna ini dengan cara ini. Informasi yang dilacak untuk bagian ini di panel temuan meliputi:

- Username — Pengguna yang memanggil Kubernetes API yang terkait dengan temuan tersebut.
- Nama Pengguna yang Ditiru - Pengguna yang ditiru oleh. `username`
- Namespace — Namespace Kubernetes di dalam klaster Amazon EKS tempat aksi terjadi.
- User Agent — Agen pengguna yang terkait dengan panggilan API Kubernetes. Agen pengguna adalah metode yang digunakan untuk melakukan panggilan seperti`kubectl`.
- API — Kubernetes API yang dipanggil oleh di `username` dalam klaster Amazon EKS.
- Informasi ASN — Informasi ASN, seperti Organisasi dan ISP, terkait dengan alamat IP pengguna yang melakukan panggilan ini.
- Hari dalam seminggu — Hari dalam seminggu ketika panggilan API Kubernetes dilakukan.
- Izin — Kata kerja Kubernetes dan sumber daya yang diperiksa untuk mengindikasikan apakah Kubernetes `username` dapat menggunakan API Kubernetes atau tidak.
- Nama Akun Layanan — Akun layanan yang terkait dengan beban kerja Kubernetes yang memberikan identitas pada beban kerja.
- Registry — Registry container yang terkait dengan image container yang di-deploy dalam beban kerja Kubernetes.
- Image - Gambar kontainer, tanpa tag dan intisari terkait, yang digunakan dalam beban kerja Kubernetes.
- Image Prefix Config - Awalan gambar dengan konfigurasi keamanan kontainer dan beban kerja diaktifkan, `hostNetwork` seperti `privileged` atau, untuk wadah yang menggunakan gambar.
- Nama Subjek — Subjek, seperti `usergroup`,, atau `serviceAccountName` yang terikat pada peran referensi dalam `RoleBinding` atau`ClusterRoleBinding`.
- Nama Peran — Nama peran yang terlibat dalam pembuatan atau modifikasi peran atau `roleBinding` API.

Anomali berbasis volume S3

Bagian ini merinci informasi kontekstual untuk anomali berbasis volume S3. Temuan berbasis volume (Exfiltration:S3/AnomalousBehavior) memantau jumlah panggilan API S3 yang tidak biasa yang dilakukan ke bucket S3 oleh pengguna, menunjukkan potensi eksfiltrasi data. Panggilan API S3 berikut dipantau untuk deteksi anomali berbasis volume.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Metrik berikut akan membantu membangun dasar perilaku biasa saat entitas IAM mengakses bucket S3. Untuk mendeteksi eksfiltrasi data, temuan deteksi anomali berbasis volume mengevaluasi semua aktivitas terhadap garis dasar perilaku yang biasa. Pilih Perilaku historis di bagian Perilaku Tidak Biasa (Identitas Pengguna), Volume yang Diamati (Identitas Pengguna), dan Volume Teramati (Bucket) untuk melihat metrik berikut.

- Jumlah panggilan `s3-api-name` API yang dipanggil oleh pengguna IAM atau peran IAM (tergantung pada panggilan mana yang dikeluarkan) terkait dengan bucket S3 yang terpengaruh selama 24 jam terakhir.
- Jumlah panggilan `s3-api-name` API yang dipanggil oleh pengguna IAM atau peran IAM (tergantung pada mana yang dikeluarkan) yang terkait dengan semua bucket S3 selama 24 jam terakhir.
- Jumlah panggilan `s3-api-name` API di semua pengguna IAM atau peran IAM (tergantung pada mana yang dikeluarkan) terkait dengan bucket S3 yang terpengaruh selama 24 jam terakhir.

Anomali berbasis aktivitas login RDS

Bagian ini merinci jumlah upaya login yang dilakukan oleh aktor yang tidak biasa dan dikelompokkan berdasarkan hasil upaya login. Jenis temuan Perlindungan RDSMengidentifikasi perilaku anomali dengan memantau peristiwa login untuk pola yang tidak biasa`successfulLoginCount`,`failedLoginCount`, dan. `incompleteConnectionCount`

- sukses LoginCount — Penghitung ini mewakili jumlah koneksi yang berhasil (kombinasi atribut login yang benar) yang dibuat ke instance database oleh aktor yang tidak biasa. Atribut login termasuk nama pengguna, kata sandi, dan nama database.
- gagal LoginCount — Penghitung ini mewakili jumlah upaya login gagal (gagal) yang dilakukan untuk membuat koneksi ke instance database. Ini menunjukkan bahwa satu atau lebih atribut dari kombinasi login, seperti nama pengguna, kata sandi, atau nama database tidak benar.
- tidak lengkap ConnectionCount — Penghitung ini mewakili jumlah upaya koneksi yang tidak dapat diklasifikasikan sebagai berhasil atau gagal. Koneksi ini ditutup sebelum database memberikan respons. Misalnya, pemindaian port di mana port database terhubung tetapi tidak ada informasi

yang dikirim ke database, atau koneksi dibatalkan sebelum login selesai dalam upaya yang berhasil atau gagal.

Anomali berbasis aktivitas data RDS

Bagian ini menjelaskan aktivitas data anomali, seperti aktor yang membaca lebih banyak baris secara signifikan, atau menghapus atau menjatuhkan lebih banyak data daripada biasanya untuk database dan pengguna tersebut. Jenis temuan Perlindungan RDSMengidentifikasi perilaku anomali dengan memantau aktivitas database untuk pola yang tidak biasa dalam jumlah baris yang dibaca atau dihapus dan dalam pernyataan drop.

- `selectedRowsdan selectStatement` — Penghitung ini mewakili jumlah baris yang dikembalikan oleh `SELECT` pernyataan dan jumlah `SELECT` pernyataan yang diamati dalam aktivitas yang terkait dengan temuan.
- `deletedRowsdan deleteStatement` — Penghitung ini mewakili jumlah baris yang dihapus oleh `DELETE` pernyataan dan jumlah `DELETE` pernyataan yang diamati dalam aktivitas yang terkait dengan temuan.
- `dropStatement`Penghitung ini mewakili jumlah operasi destruktif, seperti `DROP` atau`TRUNCATE`, yang dapat menghapus objek database atau data dalam aktivitas yang terkait dengan temuan.

GuardDuty mungkin mengumpulkan telemetri aktivitas data tambahan, seperti penghitung baru, di masa depan untuk meningkatkan kemanjuran temuan aktivitas data dan memperkenalkan deteksi ancaman Perlindungan RDS baru.

GuardDuty menemukan agregasi

GuardDuty memperbarui temuan yang dihasilkan secara dinamis. Jika GuardDuty mendeteksi aktivitas baru yang terkait dengan masalah keamanan yang sama, maka alih-alih membuat temuan baru, GuardDuty akan memperbarui temuan asli dengan detail terbaru. Perilaku ini memungkinkan Anda mengidentifikasi masalah yang sedang berlangsung, tanpa perlu melihat beberapa laporan serupa, dan mengurangi volume keseluruhan temuan untuk masalah keamanan yang diketahui.

Misalnya, untuk pencarianUnauthorizedAccess:EC2/SSHBruteForce, beberapa upaya akses terhadap instans Anda akan digabungkan ke ID pencarian yang sama, sehingga meningkatkan jumlah Hitungan dalam detail temuan. Ini karena temuan tersebut mewakili satu masalah keamanan dengan instans yang menunjukkan bahwa port SSH pada instans tidak diamankan dengan benar

terhadap tipe aktivitas ini. Namun, jika GuardDuty mendeteksi aktivitas akses SSH yang menargetkan instance baru di lingkungan Anda, itu akan membuat temuan baru dengan ID penemuan unik untuk mengingatkan Anda tentang fakta bahwa ada masalah keamanan yang terkait dengan sumber daya baru.

Ketika temuan digabungkan, itu diperbarui dengan informasi dari kejadian terbaru dari aktivitas itu. Ini berarti bahwa dalam contoh di atas, jika instans Anda adalah target upaya brute force dari aktor baru, detail temuan akan diperbarui untuk mencerminkan IP jarak jauh dari sumber terbaru dan informasi lama akan diganti. Informasi lengkap tentang upaya aktivitas individual akan tetap tersedia di CloudTrail log atau Log Aliran VPC Anda.

Kriteria yang mengingatkan GuardDuty untuk menghasilkan temuan baru alih-alih menggabungkan yang sudah ada tergantung pada jenis temuan. Kriteria agregasi untuk setiap jenis temuan ditentukan oleh teknisi keamanan kami untuk memberikan gambaran umum tentang masalah keamanan yang berbeda dalam akun Anda.

Saat GuardDuty menghasilkan jenis pencarian urutan serangan di akun Anda, temuan akan digabungkan hanya ketika Anda GuardDuty mengidentifikasi sinyal serupa dalam urutan yang sama di akun Anda. Jika tidak, GuardDuty akan menghasilkan urutan serangan lain.

Mengelola GuardDuty temuan Amazon

GuardDuty menawarkan beberapa fitur penting untuk membantu Anda mengurutkan, menyimpan, dan mengelola temuan Anda. Fitur-fitur ini akan membantu Anda menyesuaikan temuan dengan lingkungan spesifik Anda, mengurangi kebisingan dari temuan bernilai rendah, dan membantu Anda fokus pada ancaman terhadap AWS lingkungan unik Anda. Tinjau topik di halaman ini untuk memahami bagaimana Anda dapat menggunakan fitur ini untuk meningkatkan nilai temuan keamanan di lingkungan Anda.

Topik:

Dasbor ringkasan di Amazon GuardDuty

Pelajari tentang komponen dasbor ringkasan yang tersedia di GuardDuty konsol.

Penyaringan temuan di GuardDuty

Pelajari cara memfilter GuardDuty temuan berdasarkan kriteria yang Anda tentukan.

Aturan penindasan di GuardDuty

Pelajari cara memfilter temuan secara otomatis yang GuardDuty memberi tahu Anda melalui aturan penekanan. Aturan penekanan mengarsipkan temuan secara otomatis berdasarkan filter.

Menyesuaikan deteksi ancaman dengan daftar entitas dan daftar alamat IP

Sesuaikan lingkup GuardDuty pemantauan menggunakan Daftar IP dan Daftar Ancaman berdasarkan alamat IP yang dapat dirutekan secara publik. Daftar IP tepercaya mencegah temuan non-DNS dihasilkan dari IP yang Anda anggap tepercaya, sementara Daftar Intel Ancaman akan mengingatkan Anda tentang aktivitas dari IP yang ditentukan pengguna. GuardDuty

Mengekspor temuan yang dihasilkan ke Amazon S3

Ekspor temuan yang dihasilkan ke bucket Amazon S3 sehingga Anda dapat menyimpan catatan melewati periode retensi temuan 90 hari di. GuardDuty Gunakan data historis ini untuk melacak potensi aktivitas mencurigakan di akun Anda dan mengevaluasi apakah langkah-langkah perbaikan yang disarankan berhasil.

Memproses GuardDuty temuan dengan Amazon EventBridge

Siapkan notifikasi otomatis untuk GuardDuty temuan melalui EventBridge acara Amazon. Anda juga dapat mengotomatiskan tugas-tugas lain EventBridge untuk membantu Anda menanggapi temuan.

Memahami CloudWatch Log dan alasan melewatkan sumber daya selama Perlindungan Malware untuk pemindaian EC2

Pelajari cara mengaudit CloudWatch Log untuk Perlindungan GuardDuty Malware untuk EC2 dan alasan mengapa instans Amazon EC2 yang terkena dampak atau volume Amazon EBS mungkin telah dilewati selama proses pemindaian.

Melaporkan positif palsu dalam Perlindungan Malware untuk EC2

Pelajari cara melaporkan potensi deteksi ancaman positif palsu di Perlindungan Malware untuk EC2.

Melaporkan hasil pemindaian objek S3 sebagai positif palsu dalam Perlindungan Malware untuk S3

Pelajari cara melaporkan potensi deteksi ancaman positif palsu di Perlindungan Malware untuk S3.

Melaporkan positif palsu dalam Perlindungan Malware untuk Backup

Pelajari cara melaporkan potensi deteksi ancaman positif palsu di Perlindungan Malware untuk Pencadangan.

Dasbor ringkasan di Amazon GuardDuty

Dasbor GuardDuty Ringkasan memberikan tampilan agregat dari GuardDuty temuan yang dihasilkan Akun AWS di Anda saat ini Wilayah AWS.

Jika Anda menggunakan akun GuardDuty administrator, dasbor menyediakan statistik dan data gabungan untuk akun dan akun anggota di organisasi Anda.

Melihat dasbor Ringkasan

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

   GuardDuty menampilkan dasbor Ringkasan secara default saat Anda membuka konsol.
2. Pada halaman Ringkasan, pilih yang diinginkan Wilayah AWS dari pemilih Wilayah di sudut kanan atas konsol.

3. Dari menu pemilih rentang tanggal, pilih rentang tanggal yang ingin Anda lihat ringkasannya. Secara default, dasbor menampilkan data untuk hari ini, Hari ini.

> **Note**
>
> Jika tidak ada temuan yang dihasilkan selama rentang tanggal yang dipilih, dasbor tidak akan memiliki data apa pun untuk ditampilkan. Anda dapat menyegarkan dasbor, atau menyesuaikan rentang tanggal.

Topik

- Ikhtisar
- Temuan
- Jenis temuan yang paling umum
- Temuan berdasarkan tingkat keparahan
- Akun dengan sebagian besar temuan
- Sumber daya dengan temuan
- Temuan yang paling tidak terjadi
- Cakupan rencana perlindungan

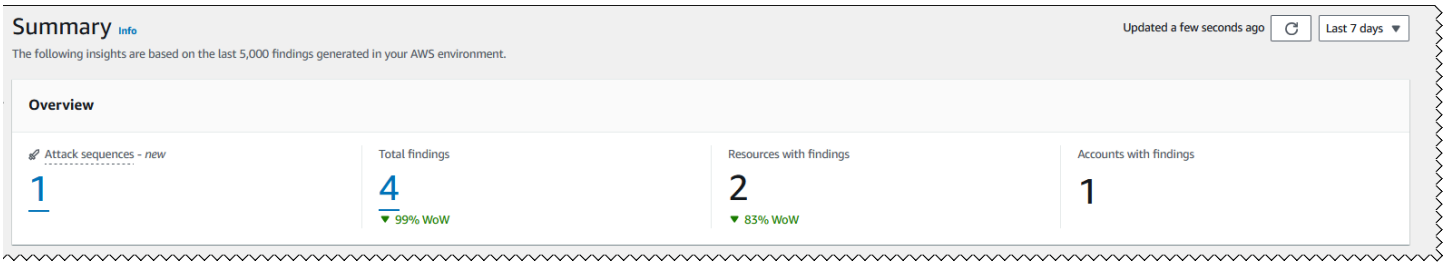
Ikhtisar

Bagian ini menyediakan data berikut:

- Urutan serangan: Menunjukkan jumlah temuan urutan serangan yang GuardDuty dihasilkan di akun Anda di Wilayah saat ini.

  GuardDuty mendeteksi potensi serangan multi-tahap di akun Anda. Anda dapat memilih nomor di bawah Urutan serangan untuk melihat detailnya di halaman Temuan.
- Total temuan: Menunjukkan jumlah total temuan yang dihasilkan di akun Anda di Wilayah saat ini. Ini termasuk temuan individu dan temuan urutan serangan.
- Sumber daya dengan temuan: Menunjukkan jumlah sumber daya yang terkait dengan temuan, dan berpotensi dikompromikan.
- Akun dengan temuan: Menunjukkan jumlah akun di mana setidaknya satu temuan dihasilkan. Jika Anda adalah akun mandiri, nilai di bidang ini adalah 1.

Untuk rentang waktu 7 hari terakhir dan 30 hari terakhir, panel Ikhtisar dapat menunjukkan perbedaan persentase dalam temuan yang dihasilkan minggu ke minggu (WoW) atau bulan ke bulan (MoM), masing-masing. Jika tidak ada temuan yang dihasilkan pada minggu atau bulan sebelumnya, maka tanpa data untuk membandingkan, perbedaan persentase mungkin tidak tersedia.



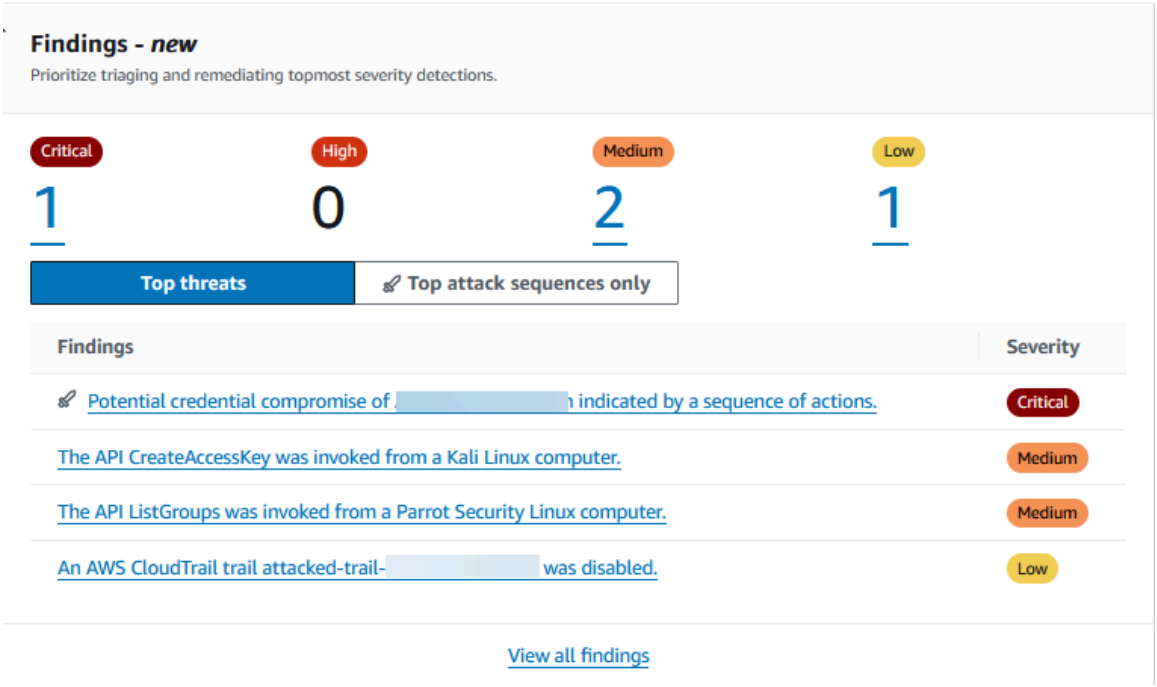
Jika Anda adalah akun GuardDuty administrator, semua bidang ini menyediakan data yang diringkas di semua akun anggota di organisasi Anda.

Temuan

Widget Temuan menampilkan hingga delapan temuan teratas. Temuan ini terdaftar berdasarkan tingkat keparahannya, dengan temuan kritis ditampilkan terlebih dahulu.

Secara default, Anda dapat melihat semua temuan. Untuk hanya melihat data temuan urutan serangan, aktifkan urutan serangan Top saja.

Dalam daftar ini, Anda dapat memilih temuan apa pun untuk melihat detailnya.



Jenis temuan yang paling umum

Bagian ini menyediakan diagram lingkaran yang menggambarkan lima jenis temuan paling umum yang dihasilkan di Wilayah saat ini. Saat mengarahkan kursor ke setiap sektor diagram lingkaran, Anda dapat mengamati hal-hal berikut:

- Jumlah temuan: Menunjukkan berapa kali temuan ini dihasilkan dalam rentang tanggal yang dipilih.
- Keparahan: Menunjukkan tingkat keparahan temuan.
- Persentase: Menunjukkan proporsi jenis temuan ini relatif terhadap total.
- Terakhir dihasilkan: Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan ini terakhir terdeteksi.

Temuan berdasarkan tingkat keparahan

Bagian ini menampilkan diagram batang yang menunjukkan jumlah total temuan selama rentang tanggal yang dipilih. Bagan memecah temuan berdasarkan tingkat keparahan (Kritis, Tinggi, Sedang, dan Rendah), dan membantu Anda melihat jumlah temuan untuk tanggal tertentu dalam kisaran tersebut.

Untuk melihat hitungan untuk setiap tingkat keparahan pada tanggal tertentu, arahkan kursor ke bilah yang sesuai di bagan.

Akun dengan sebagian besar temuan

Bagian ini menyediakan data berikut:

- Akun: Menunjukkan Akun AWS ID tempat temuan dibuat.
- Hitungan temuan: Menunjukkan berapa kali temuan dibuat untuk ID akun ini.
- Terakhir dihasilkan: Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan terakhir dibuat untuk ID akun ini.
- Filter keparahan: Secara default, data ditampilkan untuk jenis temuan tingkat keparahan tinggi. Opsi yang memungkinkan untuk bidang ini adalah Semua tingkat keparahan, Tingkat keparahan kritis, Tingkat keparahan tinggi, dan Tingkat keparahan sedang.

Sumber daya dengan temuan

Bagian ini menyediakan data berikut:

- Sumber Daya: Menampilkan jenis sumber daya yang berpotensi terpengaruh dan jika sumber daya ini milik akun Anda, Anda dapat mengakses tautan cepat untuk melihat detail sumber daya. Jika Anda adalah akun GuardDuty administrator, Anda dapat melihat detail sumber daya yang berpotensi terkena dampak dengan mengakses GuardDuty konsol dengan kredensil akun anggota pemilik.
- Akun: Menunjukkan Akun AWS ID tempat sumber daya ini berada.
- Hitungan temuan: Menunjukkan berapa kali sumber daya ini dikaitkan dengan temuan.
- Terakhir dihasilkan: Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan yang terkait dengan sumber daya ini terakhir dihasilkan.
- Filter tipe sumber daya: Secara default, data ditampilkan untuk semua jenis sumber daya. Dengan menggunakan filter ini, Anda dapat memilih untuk melihat data untuk jenis sumber daya tertentu, seperti Instance, AccessKey, Lambda, dan lainnya.
- Filter keparahan: Secara default, data ditampilkan untuk Semua tingkat keparahan. Dengan menggunakan filter ini, Anda dapat memilih untuk melihat data untuk tingkat keparahan lainnya. Pilihan yang mungkin adalah Tingkat keparahan kritis, Tingkat keparahan tinggi, tingkat keparahan sedang, dan Semua tingkat keparahan.

Temuan yang paling tidak terjadi

Bagian ini menyoroti menemukan jenis yang jarang terjadi di AWS lingkungan Anda. Widget ini dirancang untuk membantu Anda mengidentifikasi dan menyelidiki potensi pola ancaman yang muncul.

Widget ini menampilkan data berikut:

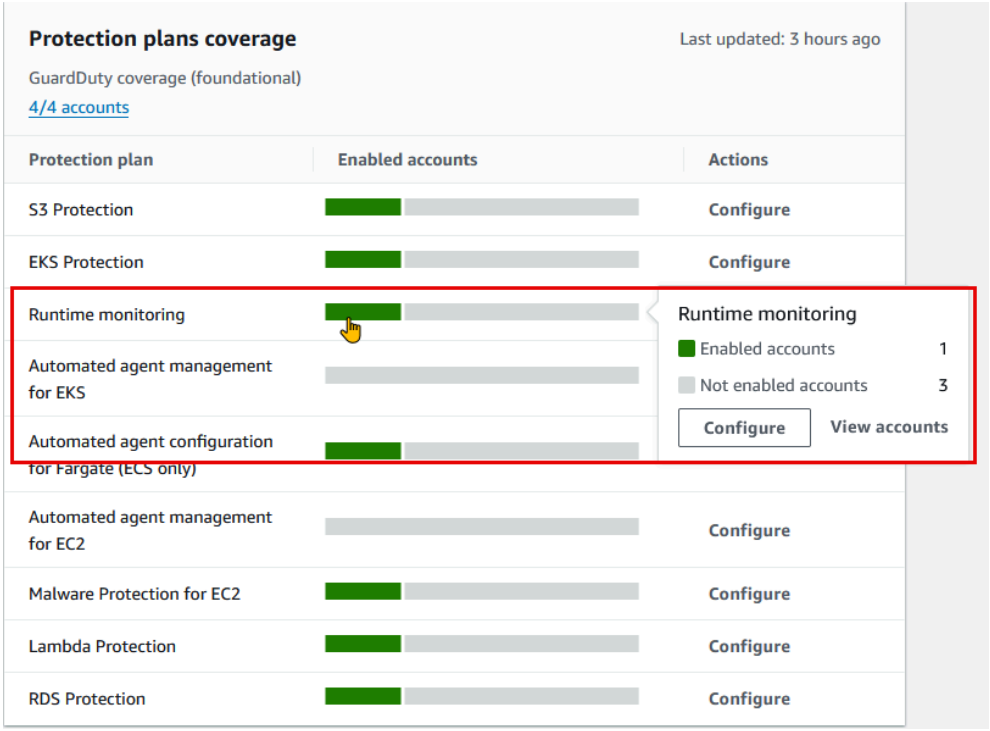
- Jenis pencarian: Menunjukkan nama tipe temuan.
- Hitungan temuan: Menunjukkan berapa kali jenis temuan ini dihasilkan dalam rentang waktu yang dipilih.
- Terakhir dihasilkan: Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan ini terakhir dihasilkan.
- Filter keparahan: Secara default, data ditampilkan untuk jenis temuan tingkat keparahan tinggi. Opsi yang memungkinkan untuk bidang ini adalah Tingkat keparahan kritis, Tingkat keparahan tinggi, Tingkat keparahan sedang, dan Semua tingkat keparahan.

Cakupan rencana perlindungan

Bagian ini menampilkan statistik untuk akun anggota di organisasi Anda. Ini menunjukkan jumlah akun anggota yang telah diaktifkan GuardDuty (deteksi ancaman dasar) di Wilayah saat ini. Hanya GuardDuty administrator yang didelegasikan yang dapat melihat statistik untuk akun anggota dalam organisasi mereka. Saat Anda membuat AWS organisasi baru, mungkin diperlukan waktu hingga 24 jam untuk menghasilkan statistik untuk seluruh organisasi.

Cara menggunakan widget ini

- Konfigurasi: Jika rencana perlindungan tidak dikonfigurasi, pilih Konfigurasi di bawah kolom Tindakan.
- Melihat akun yang diaktifkan: Arahkan kursor ke bilah di kolom Akun yang diaktifkan untuk melihat berapa banyak akun yang telah mengaktifkan setiap paket perlindungan. Untuk melihat detail akun lebih lanjut, pilih bilah hijau, dan pilih Lihat akun.



Penyaringan temuan di GuardDuty

Filter temuan memungkinkan Anda melihat temuan yang sesuai dengan kriteria yang Anda tentukan dan memfilter temuan yang tidak sesuai. Anda dapat dengan mudah membuat filter pencarian menggunakan GuardDuty konsol Amazon, atau Anda dapat membuatnya dengan CreateFilterAPI

menggunakan JSON. Tinjau bagian berikut untuk memahami cara membuat filter di konsol. Untuk menggunakan filter ini untuk mengarsipkan temuan yang masuk secara otomatis, lihatAturan penindasan di GuardDuty.

Saat Anda membuat filter, pertimbangkan daftar berikut:

- Anda dapat menentukan minimum satu atribut dan maksimum hingga 50 atribut sebagai kriteria untuk filter tertentu.
- Saat Anda menggunakan operator Sama atau Tidak sama dengan untuk memfilter nilai atribut, seperti ID Akun, Anda dapat menentukan maksimum 50 nilai.
- Setiap atribut kriteria filter dievaluasi sebagai operator `AND`. Beberapa nilai untuk atribut yang sama dievaluasi sebagai `AND/OR`.
- Untuk informasi tentang jumlah maksimum filter tersimpan yang dapat Anda buat Akun AWS di masing-masing filter Wilayah AWS, lihatGuardDuty kuota.
- `service.additionalInfo`Bidang di bawah ditentukan menggunakan jalur JSON lengkapnya, sama seperti bidang lainnya. Sebagai contoh: `{ "service.additionalInfo.sample": { "Equals": ["true"] } }`.
- Bidang stempel waktu menerima nilai dalam format milidetik Unix Epoch (misalnya,). `1486685375000` Untuk daftar lengkap bidang stempel waktu, lihat catatan di bawah ini.

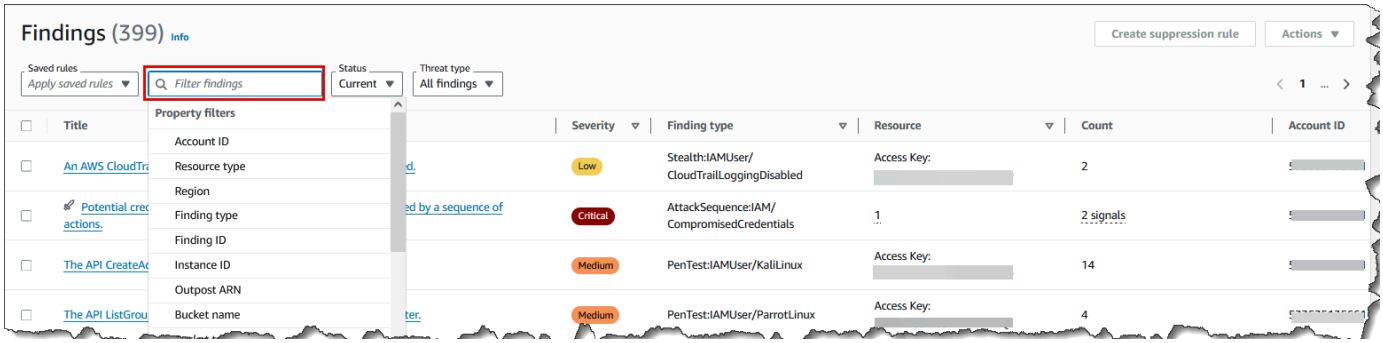
Bagian berikut memberikan petunjuk tentang cara membuat dan menyimpan filter menggunakan GuardDuty konsol, dan perintah API dan CLI. Pilih metode akses pilihan Anda untuk melanjutkan.

Membuat dan menyimpan set filter di GuardDuty konsol

Filter pencarian dapat dibuat dan diuji melalui GuardDuty konsol. Anda dapat menyimpan filter yang dibuat melalui konsol untuk digunakan dalam aturan penekanan atau operasi filter mendatang. Filter terbuat dari setidaknya satu kriteria filter. Terdiri dari satu atribut filter yang dipasangkan dengan setidaknya satu nilai.

Untuk membuat dan menyimpan kriteria filter (konsol)

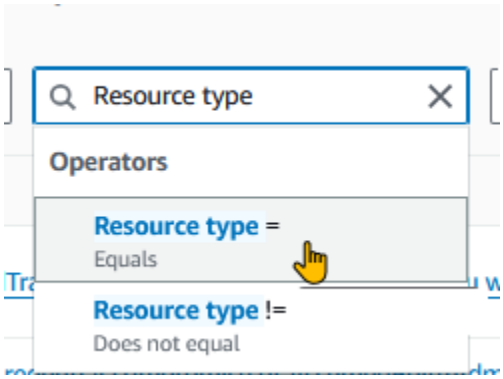
1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi kiri, pilih Temuan.
3. Pada halaman Temuan, pilih bilah Filter temuan di sebelah menu Aturan tersimpan. Ini akan menampilkan daftar filter Properti yang diperluas.



4. Dari daftar filter yang diperluas, pilih atribut berdasarkan yang ingin Anda filter tabel temuan.

   Misalnya, untuk melihat temuan yang sumber daya yang berpotensi terkena dampak adalah S3Bucket, pilih tipe Resource.

5. Untuk Operator, pilih salah satu yang akan membantu Anda memfilter temuan untuk mendapatkan hasil yang diinginkan. Untuk melanjutkan contoh dari langkah sebelumnya, pilih Jenis sumber daya =. Ini akan menampilkan daftar jenis sumber daya di GuardDuty.



   Jika kasus penggunaan Anda mengharuskan mengecualikan temuan spesifik, Anda dapat memilih Tidak sama atau! = operator.

6. Tentukan nilai untuk filter properti yang dipilih. Jika perlu, pilih Terapkan. Untuk melanjutkan contoh dari langkah sebelumnya, Anda dapat memilih S3Bucket.

   Ini akan menampilkan temuan yang cocok dengan filter yang diterapkan.

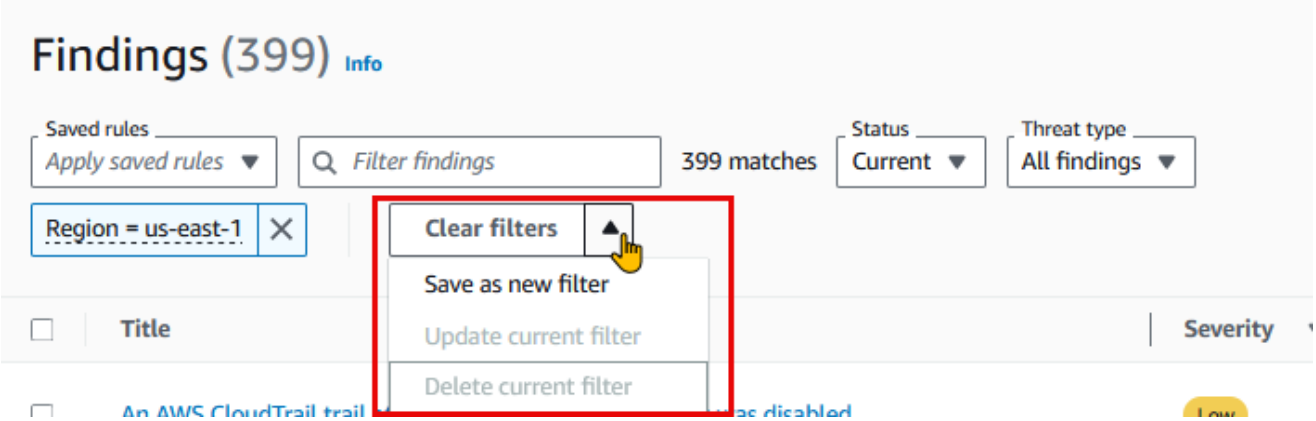
7. Untuk menambahkan lebih dari satu kriteria filter, ulangi langkah 3-6.

   Untuk daftar lengkap atribut, lihatFilter properti di GuardDuty.

8. (Opsional) simpan atribut dan nilai yang ditentukan sebagai filter

   Untuk menerapkan kombinasi filter ini lagi di masa mendatang, Anda dapat menyimpan atribut yang ditentukan dan nilainya sebagai set filter.

a. Setelah Anda membuat kriteria filter dengan satu atau beberapa filter properti, pilih panah di menu Hapus filter.



b. Masukkan nama set filter. Nama harus 3-64 karakter. Karakter yang valid adalah a-z, A-Z, 0-9, periode (.), tanda hubung (-), dan garis bawah (_).

c. Deskripsi adalah opsional. Jika Anda memasukkan deskripsi, itu dapat memiliki hingga 512 karakter.

d. Pilih Buat.

Membuat dan menyimpan set filter dengan menggunakan GuardDuty API dan CLI

Anda dapat membuat dan menguji filter temuan dengan menggunakan perintah API atau CLI. Filter terbuat dari setidaknya satu kriteria filter. Terdiri dari satu atribut filter yang dipasangkan dengan setidaknya satu nilai. Anda dapat menyimpan filter untuk membuat Aturan penekanan atau melakukan operasi filter lainnya nanti.

Untuk membuat filter pencarian menggunakan API/CLI

- Jalankan CreateFilterAPI dengan menggunakan ID detektor regional Akun AWS tempat Anda ingin membuat filter.

  Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`
- Atau, Anda dapat menggunakan CLI create-filter untuk membuat dan menyimpan filter. Anda dapat menggunakan satu atau beberapa kriteria filter dariFilter properti di GuardDuty.

Gunakan contoh berikut dengan mengganti nilai placeholder yang ditunjukkan dengan warna merah.

Contoh 1: Buat filter baru untuk melihat semua temuan yang cocok dengan jenis temuan tertentu

Contoh berikut membuat filter yang cocok dengan semua `PortScan` temuan untuk instance yang dibuat dari gambar tertentu. Nilai placeholder ditampilkan dalam warna merah. Ganti nilai-nilai ini dengan nilai yang sesuai untuk akun Anda. Misalnya, ganti *12abc34d567e8fa901bc2d34EXAMPLE* dengan ID detektor regional Anda.

```
aws guardduty create-filter \
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \
--name FilterExampleName \
--finding-criteria '{"Criterion": {"type": {"Equals": ["Recon:EC2/Portscan"]},
 "resource.instanceDetails.imageId": {"Equals":["ami-0a7a207083example"]}} }'
```

Contoh 2: Buat filter baru untuk melihat semua temuan yang cocok dengan tingkat keparahan

Contoh berikut membuat filter yang cocok dengan semua temuan yang terkait dengan `HIGH` tingkat keparahan. Nilai placeholder ditampilkan dalam warna merah. Ganti nilai-nilai ini dengan nilai yang sesuai untuk akun Anda. Misalnya, ganti *12abc34d567e8fa901bc2d34EXAMPLE* dengan ID detektor regional Anda.

```
aws guardduty create-filter \
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \
--name FilterExampleName \
--finding-criteria '{"Criterion": {"severity": {"Equals": ["7", "8"]}} }'
```

- Untuk API/CLI, Tingkat keparahan temuan direpresentasikan sebagai angka. Untuk menyaring temuan berdasarkan tingkat keparahan, gunakan nilai berikut:
  - Untuk `LOW` tingkat keparahan, gunakan `{ "severity": { "Equals": ["1", "2", "3"] } }`
  - Untuk `MEDIUM` tingkat keparahan, gunakan `{ "severity": { "Equals": ["4", "5", "6"] } }`
  - Untuk `HIGH` tingkat keparahan, gunakan `{ "severity": { "Equals": ["7", "8"] } }`
  - Untuk `CRITICAL` tingkat keparahan, gunakan `{ "severity": { "Equals": ["9", "10"] } }`

- Untuk temuan dengan beberapa tingkat keparahan, gunakan nilai placeholder yang mirip dengan contoh berikut: `{ "severity": { "Equals": ["7", "8", "9", "10"] } }`

  Contoh ini akan menunjukkan temuan yang memiliki `CRITICAL` tingkat keparahan `HIGH` atau tingkat keparahan.

  > **Note**
  >
  > Jika Anda menentukan contoh dengan hanya satu nilai numerik, bukan semua nilai numerik yang terkait dengan tingkat keparahan, API dan CLI mungkin menampilkan temuan yang difilter. Saat Anda menggunakan set filter tersimpan ini di GuardDuty konsol, itu tidak akan berfungsi seperti yang diharapkan. Ini karena GuardDuty konsol menganggap nilai filter sebagai`CRITICAL`,, `HIGHMEDIUM`, dan`LOW`. Misalnya, filter yang dibuat dengan perintah CLI yang menyertakan `{ "severity": { "Equals": ["9"] } }` diharapkan menampilkan output yang sesuai. API/CLI Namun, filter yang disimpan ini mencakup tingkat keparahan sebagian saat digunakan di GuardDuty konsol dan tidak akan menampilkan output yang diharapkan. Hal ini membuat API dan CLI perlu menentukan semua nilai yang terkait dengan setiap tingkat keparahan.

Filter metadata siklus hidup

Saat mengambil detail filter menggunakan GetFilterAPI, Anda dapat melihat bidang metadata siklus hidup. Bidang ini menunjukkan kapan filter dibuat dan berapa kali telah dimodifikasi.

GetFilterRespons mencakup bidang metadata siklus hidup berikut:

`createdAt`

Stempel waktu saat filter awalnya dibuat. GuardDuty menetapkan nilai ini pada waktu pembuatan dan tidak pernah mengubahnya. GuardDuty tidak mengisi bidang ini untuk filter lama (filter yang Anda buat sebelum fitur ini diluncurkan).

`updatedAt`

Stempel waktu saat filter terakhir diperbarui. GuardDuty memperbarui nilai ini pada setiap UpdateFilterpanggilan yang berhasil. Pada waktu pembuatan, `updatedAt` cocok`createdAt`. Untuk filter lama, bidang ini hanya muncul setelah Anda memperbarui filter setidaknya sekali.

`version`

Integer yang menghitung berapa kali Anda telah memodifikasi filter. Ini dimulai pada 1 saat Anda membuat filter dan meningkat 1 dengan setiap UpdateFilter panggilan yang berhasil, terlepas dari apakah konten filter berubah. GuardDuty tidak mengisi bidang ini untuk filter lama.

> **Note**
>
> Bidang metadata siklus hidup ini hanya-baca. UpdateFilterOperasi CreateFilter dan tidak menerima bidang ini sebagai masukan, dan tanggapan mereka tidak termasuk bidang ini. Untuk melihat metadata siklus hidup, panggil. GetFilter

Filter properti di GuardDuty

Apabila Anda membuat filter atau mengurutkan temuan menggunakan operasi API, Anda harus menentukan kriteria filter di JSON. Kriteria filter ini berkorelasi dengan detail JSON temuan. Tabel berikut berisi daftar nama tampilan konsol untuk atribut filter dan nama bidang JSON setaranya.

Nama bidang konsol	Nama bidang JSON
account-id	accountId
ID Temuan	id
Region	region
Kepelikan	kepelikan Anda dapat memfilter jenis temuan berdasark an tingkat keparahan jenis temuan. Untuk informasi lebih lanjut tentang nilai tingkat keparahan, lihatTingkat keparahan GuardDuty temuan. Jika Anda menggunakan `severity` dengan API, AWS CLI, atau CloudForm ation, itu diberi nilai numerik. Untuk informasi selengkapnya, lihat FindingCriteria di Referensi Amazon GuardDuty API.

Nama bidang konsol	Nama bidang JSON
Tipe temuan	jenis
Nama aturan deteksi kustom	kustom DetectionRuleName Hadir hanya pada temuan yang dihasilkan oleh Runtime Monitoring Custom Detection Rule. Untuk informasi selengkapnya, lihat Temuan dari aturan Runtime Monitoring.
Diperbarui pada	updatedAt
Access key ID	resource.access KeyDetails.accessKeyId
ID principal	resource.access KeyDetails.principalId
nama pengguna	resource.access KeyDetails.userName
Jenis pengguna	resource.access KeyDetails.userType
ID profil instans IAM	resource.instance Details.iamInstanceProfile.id
ID Instans	resource.instance Details.instanceId
ID citra instans	resource.instance Details.imageId
Kunci tag contoh	resource.instance Details.tags.key
Nilai tag instance	resource.instance Details.tags.value
Alamat IPv6	resource.instance Details.networkInterfaces.ipv6Addresses
Alamat IPv4 privat	resource.instance Details.networkInterfaces.privateIpAddresses.privateIpAddress
Nama DNS publik	resource.instance Details.networkInterfaces.publicDnsName

Nama bidang konsol	Nama bidang JSON
IP Publik	resource.instance Details.networkInterfaces.publicIp
ID grup keamanan	resource.instance Details.networkInterfaces.securityGroups.groupId
Nama grup keamanan	resource.instance Details.networkInterfaces.securityGroups.groupName
ID Subnet	resource.instance Details.networkInterfaces.subnetId
VPC ID	resource.instance Details.networkInterfaces.vpcId
ARN Outpost	resource.instance Details.outpostARN
Tipe sumber daya	resource.resourceType
Izin bucket	sumber daya.s3 BucketDetails.publicAccess.effectivePermission
Nama Bucket	sumber daya.s3 BucketDetails.name
Kunci tanda bucket	sumber daya.s3 BucketDetails.tags.key
Nilai tanda bucket	sumber daya.s3 BucketDetails.tags.value
Jenis bucket	sumber daya.s3 BucketDetails.type
Tipe tindakan	service.action.actionType
Panggilan API	service.action.aws ApiCallAction.api
Tipe pemanggil API	service.action.aws ApiCallAction.callerType
Kode Kesalahan API	service.action.aws ApiCallAction.errorCode

Nama bidang konsol	Nama bidang JSON
Kota pemanggil API	service.action.aws ApiCallAction.remoteIpDetails.city.cityName
Negara pemanggil API	service.action.aws ApiCallAction.remoteIpDetails.country.countryName
Alamat IPv4 pemanggil API	service.action.aws ApiCallAction.remoteIpDetails.ipAddressV4
Alamat IPv6 pemanggil API	service.action.aws ApiCallAction.remoteIpDetails.ipAddressV6
ID ASN pemanggil API	service.action.aws ApiCallAction.remoteIpDetails.organization.asn
Nama ASN pemanggil API	service.action.aws ApiCallAction.remoteIpDetails.organization.asnOrg
Nama layanan pemanggil API	service.action.aws ApiCallAction.serviceName
Domain permintaan DNS	service.action.dns RequestAction.domain
Akhiran domain permintaan DNS	service.action.dns RequestAction.domainWithSuffix
Koneksi jaringan diblokir	service.action.network ConnectionAction.blocked
Arah koneksi jaringan	service.action.network ConnectionAction.connectionDirection
Port lokal koneksi jaringan	service.action.network ConnectionAction.localPortDetails.port
Protokol koneksi jaringan	service.action.network ConnectionAction.protocol

Nama bidang konsol	Nama bidang JSON
Kota koneksi jaringan	service.action.network ConnectionAction.remoteIpDetails.city.cityName
Negara koneksi jaringan	service.action.network ConnectionAction.remoteIpDetails.country.countryName
Alamat IPv4 jarak jauh koneksi jaringan	service.action.network ConnectionAction.remoteIpDetails.ipAddressV4
Koneksi jaringan alamat IPv6 jarak jauh	service.action.network ConnectionAction.remoteIpDetails.ipAddressV6
ID ASN IP jarak jauh koneksi jaringan	service.action.network ConnectionAction.remoteIpDetails.organization.asn
Nama ASN IP jarak jauh koneksi jaringan	service.action.network ConnectionAction.remoteIpDetails.organization.asnOrg
Port jarak jauh koneksi jaringan	service.action.network ConnectionAction.remotePortDetails.port
Akun jarak jauh berafiliasi	service.action.aws ApiCallAction.remoteAccountDetails.affiliated
Alamat IPv4 pemanggil API Kubernetes	service.action.kubernetes ApiCallAction.remoteIpDetails.ipAddressV4
Alamat IPv6 pemanggil API Kubernetes	service.action.kubernetes ApiCallAction.remoteIpDetails.ipAddressV6
Namespace Kubernetes	service.action.kubernetes ApiCallAction.namespace
ID ASN pemanggil API Kubernetes	service.action.kubernetes ApiCallAction.remoteIpDetails.organization.asn
URI permintaan panggilan API Kubernetes	service.action.kubernetes ApiCallAction.requestUri

Nama bidang konsol	Nama bidang JSON
Kode status API Kubernetes	service.action.kubernetes ApiCallAction.statusCode
Koneksi jaringan alamat IPv4 lokal	service.action.network ConnectionAction.localIpDetails.ipAddressV4
Koneksi jaringan alamat IPv6 lokal	service.action.network ConnectionAction.localIpDetails.ipAddressV6
Protokol	service.action.network ConnectionAction.protocol
Nama layanan panggilan API	service.action.aws ApiCallAction.serviceName
ID akun pemanggil API	service.action.aws ApiCallAction.remoteAccountDetails.accountId
Nama daftar ancaman	layanan.tambahan Info.threatListName
Peran sumber daya	service.resourceRole
Nama cluster EKS	sumber daya.eks ClusterDetails.name
Nama beban kerja Kubernetes	resource.kubernetes Details.kubernetes WorkloadDetails.name
Namespace beban kerja Kubernetes	resource.kubernetes Details.kubernetes WorkloadDetails.namespace
Nama pengguna Kubernetes	resource.kubernetes Details.kubernetes UserDetails.username
Gambar kontainer Kubernetes	resource.kubernetes Details.kubernetes WorkloadDetails.containers.image
Awalan gambar kontainer Kubernetes	resource.kubernetes Details.kubernetes WorkloadDetails.containers.imagePrefix

Nama bidang konsol	Nama bidang JSON
Pindai ID	service.ebs VolumeScanDetails.scanId
Nama ancaman pemindaian volume EBS	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.name
Nama ancaman pemindaian objek S3	layanan.malware ScanDetails.threats.name
Tingkat keparahan ancaman	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.severity
Berkas SHA	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.hash
Nama cluster ECS	sumber daya.ecs ClusterDetails.name
Gambar kontainer ECS	sumber daya.ecs ClusterDetails.taskDetails.containers.image
Definisi tugas ECS ARN	sumber daya.ecs ClusterDetails.taskDetails.definitionArn
Gambar wadah mandiri	resource.container Details.image
Id Instans Database	resource.rds DbInstanceDetails.dbInstanceIdentifier
Id Kluster Basis Data	resource.rds DbInstanceDetails.dbClusterIdentifier
Mesin basis data	resource.rds DbInstanceDetails.engine
Pengguna basis data	resource.rds DbUserDetails.user
Dapat dieksekusi SHA-256	service.runtime Details.process.executableSha256

Nama bidang konsol	Nama bidang JSON
Nama proses	service.runtime Details.process.name
Jalur yang dapat dieksekusi	service.runtime Details.process.executablePath
Nama fungsi Lambda	sumber daya.lambda Details.functionName
Fungsi Lambda ARN	sumber daya.lambda Details.functionArn
Tombol tag fungsi Lambda	sumber daya.lambda Details.tags.key
Nilai tag fungsi Lambda	sumber daya.lambda Details.tags.value
Domain permintaan DNS	service.action.dns RequestAction.domainWithSuffix

Semua bidang temuan lainnya (tercantum di bawah) hanya tersedia sebagai kriteria filter aturan penekanan (menggunakan CreateFilterdan UpdateFilter). Bidang ini tidak didukung oleh operasi API lainnya. Aturan penindasan yang menggunakan bidang ini harus dibuat atau diperbarui melalui API. Bidang ini hanya dapat diterapkan untuk filter dengan `ARCHIVE` tindakan.

> **Note**
>
> Bidang berikut menerima nilai stempel waktu dalam format milidetik Unix Epoch (misalnya, `1262309025000` mewakili Jumat, 1 Januari 2010 pukul 1:23:45 GMT):
>
> - CREATEDAT
> - updatedAt
> - service.event FirstSeen
> - service.event LastSeen
> - resource.instance Details.launchTime
> - sumber daya.lambda Details.lastModifiedAt
> - sumber daya.s3 BucketDetails.createdAt
> - sumber daya.eks ClusterDetails.createdAt
> - sumber daya.ecs ClusterDetails.taskDetails.createdAt
> - sumber daya.ecs ClusterDetails.taskDetails.startedAt
> - service.ebs VolumeScanDetails.scanStartedAt

- service.ebs VolumeScanDetails.scanCompletedAt
- service.runtime Details.context.modifiedAt
- service.runtime Details.context.modifyingProcess.startTime
- service.runtime Details.context.modifyingProcess.lineage.startTime
- service.runtime Details.context.targetProcess.startTime
- service.runtime Details.context.targetProcess.lineage.startTime
- service.runtime Details.process.startTime
- service.runtime Details.process.lineage.startTime
- Service.detection.sequence.actors.session.createdTime
- Service.detection.sequence.signals.createdat
- Service.detection.sequence.signals.updateDat
- service.detection.sequence.signals.first SeenAt
- service.detection.sequence.signals.last SeenAt
- service.detection.sequence.resources.data.s3 Bucket.createdAt
- service.detection.sequence.resources.data.ecs Task.createdAt
- service.detection.sequence.resources.data.eks Cluster.createdAt

Nama bidang JSON
arn
terkait AttackSequenceArn
CREATEDAT
partisi
resource.access KeyDetails.userIdentity.accessKeyId
resource.access KeyDetails.userIdentity.accountId
resource.access KeyDetails.userIdentity.arn
resource.access KeyDetails.userIdentity.principalId
resource.access KeyDetails.userIdentity.sessionContext.attributes.mfaAuthenticated
resource.access KeyDetails.userIdentity.sessionContext.ec2RoleDelivery

Nama bidang JSON
resource.access KeyDetails.userIdentity.sessionContext.invokedBy
resource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.accountId
resource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.arn
resource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.principalId
resource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.type
resource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.userName
resource.access KeyDetails.userIdentity.sessionContext.sourceIdentity
resource.access KeyDetails.userIdentity.sessionContext.webIdFederationData.attributes
resource.access KeyDetails.userIdentity.sessionContext.webIdFederationData.federatedProvider
resource.access KeyDetails.userIdentity.type
resource.access KeyDetails.userIdentity.userName
sumber daya.bedrock GuardrailDetails.guardrailArn
sumber daya.bedrock GuardrailDetails.guardrailVersion
resource.container Details.containerRuntime
resource.container Details.imagePrefix
resource.container Details.securityContext.allowPrivilegeEscalation
resource.container Details.securityContext.privileged
resource.container Details.volumeMounts.mountPath
resource.container Details.volumeMounts.name
sumber daya.ebs VolumeDetails.scannedVolumeDetails.deviceName

Nama bidang JSON
sumber daya.ebs VolumeDetails.scannedVolumeDetails.encryptionType
sumber daya.ebs VolumeDetails.scannedVolumeDetails.kmsKeyArn
sumber daya.ebs VolumeDetails.scannedVolumeDetails.snapshotArn
sumber daya.ebs VolumeDetails.scannedVolumeDetails.volumeArn
sumber daya.ebs VolumeDetails.scannedVolumeDetails.volumeSizeInGB
sumber daya.ebs VolumeDetails.scannedVolumeDetails.volumeType
sumber daya.ebs VolumeDetails.skippedVolumeDetails.deviceName
sumber daya.ebs VolumeDetails.skippedVolumeDetails.encryptionType
sumber daya.ebs VolumeDetails.skippedVolumeDetails.kmsKeyArn
sumber daya.ebs VolumeDetails.skippedVolumeDetails.snapshotArn
sumber daya.ebs VolumeDetails.skippedVolumeDetails.volumeArn
sumber daya.ebs VolumeDetails.skippedVolumeDetails.volumeSizeInGB
sumber daya.ebs VolumeDetails.skippedVolumeDetails.volumeType
sumber daya.ecs ClusterDetails.activeServicesCount
sumber daya.ecs ClusterDetails.arn
sumber daya.ecs ClusterDetails.registeredContainerInstancesCount
sumber daya.ecs ClusterDetails.runningTasksCount
sumber daya.ecs ClusterDetails.status
sumber daya.ecs ClusterDetails.tags.key
sumber daya.ecs ClusterDetails.tags.value

Nama bidang JSON
sumber daya.ecs ClusterDetails.taskDetails.arn
sumber daya.ecs ClusterDetails.taskDetails.containers.containerRuntime
sumber daya.ecs ClusterDetails.taskDetails.containers.id
sumber daya.ecs ClusterDetails.taskDetails.containers.imagePrefix
sumber daya.ecs ClusterDetails.taskDetails.containers.name
sumber daya.ecs ClusterDetails.taskDetails.containers.securityContext.allowPrivilegeEscalation
sumber daya.ecs ClusterDetails.taskDetails.containers.securityContext.privileged
sumber daya.ecs ClusterDetails.taskDetails.containers.volumeMounts.mountPath
sumber daya.ecs ClusterDetails.taskDetails.containers.volumeMounts.name
sumber daya.ecs ClusterDetails.taskDetails.createdAt
sumber daya.ecs ClusterDetails.taskDetails.group
sumber daya.ecs ClusterDetails.taskDetails.launchType
sumber daya.ecs ClusterDetails.taskDetails.startedAt
sumber daya.ecs ClusterDetails.taskDetails.startedBy
sumber daya.ecs ClusterDetails.taskDetails.tags.key
sumber daya.ecs ClusterDetails.taskDetails.tags.value
sumber daya.ecs ClusterDetails.taskDetails.version
sumber daya.ecs ClusterDetails.taskDetails.volumes.hostPath.path
sumber daya.ecs ClusterDetails.taskDetails.volumes.name
sumber daya.eks ClusterDetails.arn

Nama bidang JSON
sumber daya.eks ClusterDetails.createdAt
sumber daya.eks ClusterDetails.status
sumber daya.eks ClusterDetails.tags.key
sumber daya.eks ClusterDetails.tags.value
sumber daya.eks ClusterDetails.vpcId
resource.instance Details.iamInstanceProfile.arn
resource.instance Details.instanceState
resource.instance Details.instanceType
resource.instance Details.launchTime
resource.instance Details.networkInterfaces.networkInterfaceId
resource.instance Details.networkInterfaces.privateDnsName
resource.instance Details.networkInterfaces.privateIpAddress
resource.instance Details.networkInterfaces.privateIpAddresses.privateDnsName
resource.instance Details.platform
resource.instance Details.productCodes.productCodeId
resource.instance Details.productCodes.productCodeType
resource.kubernetes Details.kubernetesUserDetails.groups
resource.kubernetes Details.kubernetesUserDetails.impersonatedUser.groups
resource.kubernetes Details.kubernetesUserDetails.impersonatedUser.username
resource.kubernetes Details.kubernetesUserDetails.sessionName

Nama bidang JSON
resource.kubernetes Details.kubernetesUserDetails.uid
resource.kubernetes Details.kubernetesWorkloadDetails.containers.containerRuntime
resource.kubernetes Details.kubernetesWorkloadDetails.containers.id
resource.kubernetes Details.kubernetesWorkloadDetails.containers.name
resource.kubernetes Details.kubernetesWorkloadDetails.containers.securityContext.allowPrivilegeEscalation
resource.kubernetes Details.kubernetesWorkloadDetails.containers.securityContext.privileged
resource.kubernetes Details.kubernetesWorkloadDetails.containers.volumeMounts.mountPath
resource.kubernetes Details.kubernetesWorkloadDetails.containers.volumeMounts.name
resource.kubernetes Details.kubernetesWorkloadDetails.hostIpc
resource.kubernetes Details.kubernetesWorkloadDetails.hostNetwork
resource.kubernetes Details.kubernetesWorkloadDetails.hostPid
resource.kubernetes Details.kubernetesWorkloadDetails.serviceAccountName
resource.kubernetes Details.kubernetesWorkloadDetails.type
resource.kubernetes Details.kubernetesWorkloadDetails.uid
resource.kubernetes Details.kubernetesWorkloadDetails.volumes.hostPath.path
resource.kubernetes Details.kubernetesWorkloadDetails.volumes.name
sumber daya.lambda Details.description
sumber daya.lambda Details.lastModifiedAt
sumber daya.lambda Details.revisionId
sumber daya.lambda Details.vpcConfig.securityGroups.groupId

Nama bidang JSON
sumber daya.lambda Details.vpcConfig.securityGroups.groupName
sumber daya.lambda Details.vpcConfig.subnetIds
sumber daya.lambda Details.vpcConfig.vpcId
resource.rds DbInstanceDetails.dbInstanceArn
resource.rds DbInstanceDetails.dbiResourceId
resource.rds DbInstanceDetails.dbSecurityGroups.name
resource.rds DbInstanceDetails.dbSecurityGroups.status
resource.rds DbInstanceDetails.engineVersion
resource.rds DbInstanceDetails.iamDatabaseAuthenticationEnabled
resource.rds DbInstanceDetails.publiclyAccessible
resource.rds DbInstanceDetails.vpcId
resource.rds DbInstanceDetails.vpcSecurityGroups.status
resource.rds DbInstanceDetails.vpcSecurityGroups.vpcSecurityGroupId
resource.rds DbUserDetails.application
resource.rds DbUserDetails.authMethod
resource.rds DbUserDetails.database
resource.rds DbUserDetails.ssl
resource.rds LimitlessDbDetails.dbClusterIdentifier
resource.rds LimitlessDbDetails.dbShardGroupArn
resource.rds LimitlessDbDetails.dbShardGroupIdentifier

Nama bidang JSON
resource.rds LimitlessDbDetails.dbShardGroupResourceId
resource.rds LimitlessDbDetails.engine
resource.rds LimitlessDbDetails.engineVersion
resource.rds LimitlessDbDetails.tags.key
resource.rds LimitlessDbDetails.tags.value
sumber daya.s3 BucketDetails.arn
sumber daya.s3 BucketDetails.createdAt
sumber daya.s3 BucketDetails.defaultServerSideEncryption.encryptionType
sumber daya.s3 BucketDetails.defaultServerSideEncryption.kmsMasterKeyArn
sumber daya.s3 BucketDetails.owner.id
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.blockPublicAcls
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.blockPublicPolicy
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.ignorePublicAcls
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.restrictPublicBuckets
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessControlList.allowsPublicReadAccess
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessControlList.allowsPublicWriteAccess

Nama bidang JSON
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.blockPublicAcls
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.blockPublicPolicy
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.ignorePublicAcls
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess
sumber daya.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess
sumber daya.s3 BucketDetails.s3ObjectDetails.eTag
sumber daya.s3 BucketDetails.s3ObjectDetails.hash
sumber daya.s3 BucketDetails.s3ObjectDetails.key
sumber daya.s3 BucketDetails.s3ObjectDetails.objectArn
sumber daya.s3 BucketDetails.s3ObjectDetails.versionId
schemaVersion
service.action.aws ApiCallAction.domainDetails.domain
service.action.aws ApiCallAction.remoteIpDetails.country.countryCode
service.action.aws ApiCallAction.remoteIpDetails.geoLocation.lat
service.action.aws ApiCallAction.remoteIpDetails.geoLocation.lon
service.action.aws ApiCallAction.remoteIpDetails.organization.isp

Nama bidang JSON
service.action.aws ApiCallAction.remoteIpDetails.organization.org
service.action.aws ApiCallAction.userAgent
service.action.dns RequestAction.blocked
service.action.dns RequestAction.protocol
service.action.kubernetes ApiCallAction.parameters
service.action.kubernetes ApiCallAction.remoteIpDetails.country.countryCode
service.action.kubernetes ApiCallAction.remoteIpDetails.geoLocation.lat
service.action.kubernetes ApiCallAction.remoteIpDetails.geoLocation.lon
service.action.kubernetes ApiCallAction.resource
service.action.kubernetes ApiCallAction.resourceName
service.action.kubernetes ApiCallAction.sourceIPs
service.action.kubernetes ApiCallAction.subresource
service.action.kubernetes ApiCallAction.userAgent
service.action.kubernetes ApiCallAction.verb
service.action.kubernetes PermissionCheckedDetails.allowed
service.action.kubernetes PermissionCheckedDetails.namespace
service.action.kubernetes PermissionCheckedDetails.resource
service.action.kubernetes PermissionCheckedDetails.verb
service.action.kubernetes RoleBindingDetails.kind
service.action.kubernetes RoleBindingDetails.name

Nama bidang JSON
service.action.kubernetes RoleBindingDetails.roleRefKind
service.action.kubernetes RoleBindingDetails.roleRefName
service.action.kubernetes RoleBindingDetails.uid
service.action.kubernetes RoleDetails.kind
service.action.kubernetes RoleDetails.name
service.action.kubernetes RoleDetails.uid
service.action.network ConnectionAction.localNetworkInterface
service.action.network ConnectionAction.localPortDetails.portName
service.action.network ConnectionAction.remoteIpDetails.country.countryCode
service.action.network ConnectionAction.remoteIpDetails.geoLocation.lat
service.action.network ConnectionAction.remoteIpDetails.geoLocation.lon
service.action.network ConnectionAction.remoteIpDetails.organization.isp
service.action.network ConnectionAction.remoteIpDetails.organization.org
service.action.network ConnectionAction.remotePortDetails.portName
service.action.port ProbeAction.blocked
service.action.port ProbeAction.portProbeDetails.localIpDetails.ipAddressV4
service.action.port ProbeAction.portProbeDetails.localIpDetails.ipAddressV6
service.action.port ProbeAction.portProbeDetails.localPortDetails.port
service.action.port ProbeAction.portProbeDetails.localPortDetails.portName
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.city.cityName

Nama bidang JSON
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.country.countryCode
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.country.countryName
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lat
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lon
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.ipAddressV4
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.ipAddressV6
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.asn
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.asnOrg
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.isp
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.org
service.action.rds LoginAttemptAction.loginAttributes.application
service.action.rds LoginAttemptAction.loginAttributes.failedLoginAttempts
service.action.rds LoginAttemptAction.loginAttributes.successfulLoginAttempts
service.action.rds LoginAttemptAction.loginAttributes.user
service.action.rds LoginAttemptAction.remoteIpDetails.city.cityName
service.action.rds LoginAttemptAction.remoteIpDetails.country.countryCode
service.action.rds LoginAttemptAction.remoteIpDetails.country.countryName
service.action.rds LoginAttemptAction.remoteIpDetails.geoLocation.lat
service.action.rds LoginAttemptAction.remoteIpDetails.geoLocation.lon
service.action.rds LoginAttemptAction.remoteIpDetails.ipAddressV4

Nama bidang JSON
service.action.rds LoginAttemptAction.remoteIpDetails.ipAddressV6
service.action.rds LoginAttemptAction.remoteIpDetails.organization.asn
service.action.rds LoginAttemptAction.remoteIpDetails.organization.asnOrg
service.action.rds LoginAttemptAction.remoteIpDetails.organization.isp
service.action.rds LoginAttemptAction.remoteIpDetails.organization.org
layanan.tambahan Info.agentDetails.agentId
layanan.tambahan Info.agentDetails.agentVersion
layanan.tambahan Info.anomalies.anomalousAPIs
layanan.tambahan Info.authenticationMethod
layanan.tambahan Info.averagePacketSizeIn
layanan.tambahan Info.averagePacketSizeOut
layanan.tambahan Info.context
layanan.tambahan Info.domain
layanan.tambahan Info.inBytes
layanan.tambahan Info.localNetworkInterfaceOwner
layanan.tambahan Info.localPort
layanan.tambahan Info.outBytes
layanan.tambahan Info.packetsIn
layanan.tambahan Info.packetsOut
layanan.tambahan Info.policyArn

Nama bidang JSON
layanan.tambahan Info.policyName
layanan.tambahan Info.remotePort
layanan.tambahan Info.sample
layanan.tambahan Info.scannedPort
layanan.tambahan Info.threatFileSha256
layanan.tambahan Info.threatName
layanan.tambahan Info.totalBytesIn
layanan.tambahan Info.totalBytesOut
layanan.tambahan Info.type
layanan.tambahan Info.unusual.asnOrg
layanan.tambahan Info.unusual.port
layanan.tambahan Info.unusualProtocol
layanan.tambahan Info.userAgent.fullUserAgent
layanan.tambahan Info.userAgent.userAgentCategory
layanan.tambahan Info.value
layanan.tambahan Info.vpcOwnerAccountId
service.count
service.detection.sequence.actors.id
service.detection.sequence.actors.process.name
service.detection.sequence.actors.process.path

Nama bidang JSON
service.detection.sequence.actors.process.sha256
Service.detection.sequence.actors.session.createdTime
service.detection.sequence.actors.session.issuer
Service.detection.sequence.actors.session.mfastatus
service.detection.sequence.actors.session.uid
service.detection.sequence.actors.user.account.account
service.detection.sequence.actors.user.account.uid
Service.detection.sequence.actors.user.credentialUid
service.detection.sequence.actors.user.name
service.detection.sequence.actors.user.type
service.detection.sequence.actors.user.uid
service.detection.sequence.additional SequenceTypes
service.detection.sequence.description
service.detection.sequence.endpoints.autonomous System.name
service.detection.sequence.endpoints.autonomous System.number
service.detection.sequence.endpoints.connection.direction
service.detection.sequence.endpoints.domain
service.detection.sequence.endpoints.id
service.detection.sequence.endpoints.ip
service.detection.sequence.endpoints.location.city

Nama bidang JSON
service.detection.sequence.endpoints.location.country
service.detection.sequence.endpoints.location.lat
service.detection.sequence.endpoints.location.lon
service.detection.sequence.endpoints.port
Service.detection.sequence.resources.accountID
Service.detection.sequence.resources.cloudpartition
service.detection.sequence.resources.data.access Key.principalId
service.detection.sequence.resources.data.access Key.userName
service.detection.sequence.resources.data.access Key.userType
service.detection.sequence.resources.data.autoscaling AutoScalingGroup.ec2InstanceUids
service.detection.sequence.resources.data.cloudformation Stack.ec2InstanceUids
service.detection.sequence.resources.data.container.image
Service.detection.sequence.resources.data.container.imageuid
service.detection.sequence.resources.data.ec2 Image.ec2InstanceUids
service.detection.sequence.resources.data.ec2 Instance.availabilityZone
service.detection.sequence.resources.data.ec2 Instance.ec2NetworkInterfaceUids
service.detection.sequence.resources.data.ec2 Instance.iamInstanceProfile.arn
service.detection.sequence.resources.data.ec2 Instance.iamInstanceProfile.id
service.detection.sequence.resources.data.ec2 Instance.imageDescription
service.detection.sequence.resources.data.ec2 Instance.instanceState

Nama bidang JSON
service.detection.sequence.resources.data.ec2 Instance.instanceType
service.detection.sequence.resources.data.ec2 Instance.outpostArn
service.detection.sequence.resources.data.ec2 Instance.platform
service.detection.sequence.resources.data.ec2 Instance.productCodes.productCodeId
service.detection.sequence.resources.data.ec2 Instance.productCodes.productCodeType
service.detection.sequence.resources.data.ec2 LaunchTemplate.ec2InstanceUids
service.detection.sequence.resources.data.ec2 LaunchTemplate.version
service.detection.sequence.resources.data.ec2 NetworkInterface.ipv6Addresses
service.detection.sequence.resources.data.ec2 NetworkInterface.privateIpAddresses.privateDnsName
service.detection.sequence.resources.data.ec2 NetworkInterface.privateIpAddresses.privateIpAddress
service.detection.sequence.resources.data.ec2 NetworkInterface.publicIp
service.detection.sequence.resources.data.ec2 NetworkInterface.securityGroups.groupId
service.detection.sequence.resources.data.ec2 NetworkInterface.securityGroups.groupName
service.detection.sequence.resources.data.ec2 NetworkInterface.subNetId
service.detection.sequence.resources.data.ec2 NetworkInterface.vpcId
service.detection.sequence.resources.data.ec2 Vpc.ec2InstanceUids
service.detection.sequence.resources.data.ecs Cluster.ec2InstanceUids
service.detection.sequence.resources.data.ecs Cluster.status
service.detection.sequence.resources.data.ecs Task.containerUids

Nama bidang JSON
service.detection.sequence.resources.data.ecs Task.createdAt
service.detection.sequence.resources.data.ecs Task.launchType
service.detection.sequence.resources.data.ecs Task.taskDefinitionArn
service.detection.sequence.resources.data.eks Cluster.arn
service.detection.sequence.resources.data.eks Cluster.createdAt
service.detection.sequence.resources.data.eks Cluster.ec2InstanceUids
service.detection.sequence.resources.data.eks Cluster.status
service.detection.sequence.resources.data.eks Cluster.vpcId
service.detection.sequence.resources.data.iam InstanceProfile.ec2InstanceUids
service.detection.sequence.resources.data.iam InstanceProfile.id
service.detection.sequence.resources.data.kubernetes Workload.containerUids
service.detection.sequence.resources.data.kubernetes Workload.namespace
service.detection.sequence.resources.data.kubernetes Workload.type
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicAclAccess
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicAclIgnoreBehavior
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicBucketRestrictBehavior
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicPolicyAccess
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicAclAccess
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicAclIgnoreBehavior

Nama bidang JSON
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicBucketRestrictBehavior
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicPolicyAccess
service.detection.sequence.resources.data.s3 Bucket.createdAt
service.detection.sequence.resources.data.s3 Bucket.effectivePermission
service.detection.sequence.resources.data.s3 Bucket.encryptionKeyArn
service.detection.sequence.resources.data.s3 Bucket.encryptionType
service.detection.sequence.resources.data.s3 Bucket.ownerId
service.detection.sequence.resources.data.s3 Bucket.publicReadAccess
service.detection.sequence.resources.data.s3 Bucket.publicWriteAccess
service.detection.sequence.resources.data.s3 Bucket.s3ObjectUids
service.detection.sequence.resources.data.s3 Object.eTag
service.detection.sequence.resources.data.s3 Object.key
service.detection.sequence.resources.data.s3 Object.versionId
service.detection.sequence.resources.name
service.detection.sequence.resources.region
Service.detection.sequence.resources.resourceType
service.detection.sequence.resources.service
service.detection.sequence.resources.tags.key
service.detection.sequence.resources.tags.value
service.detection.sequence.resources.uid

Nama bidang JSON
service.detection.sequence.sequence Indicators.key
service.detection.sequence.sequence Indicators.title
service.detection.sequence.sequence Indicators.values
Service.detection.sequence.signals.actorids
service.detection.sequence.signals.count
Service.detection.sequence.signals.createdat
service.detection.sequence.signals.description
Service.detection.sequence.signals.endPointIds
service.detection.sequence.signals.first SeenAt
service.detection.sequence.signals.last SeenAt
service.detection.sequence.signals.name
Service.detection.sequence.signals.resourceUids
service.detection.sequence.signals.severity
service.detection.sequence.signals.signal Indicators.key
service.detection.sequence.signals.signal Indicators.title
service.detection.sequence.signals.signal Indicators.values
service.detection.sequence.signals.type
service.detection.sequence.signals.uid
Service.detection.sequence.signals.updateDat
service.detection.sequence.uid

Nama bidang JSON
Service.detectorID
service.ebs VolumeScanDetails.scanCompletedAt
service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.count
service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.severity
service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.threatName
service.ebs VolumeScanDetails.scanDetections.scannedItemCount.files
service.ebs VolumeScanDetails.scanDetections.scannedItemCount.totalGb
service.ebs VolumeScanDetails.scanDetections.scannedItemCount.volumes
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.itemCount
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.shortened
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.fileName
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.filePath
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.volumeArn
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.itemCount
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.uniqueThreatNameCount
service.ebs VolumeScanDetails.scanDetections.threatsDetectedItemCount.files
service.ebs VolumeScanDetails.scanStartedAt
service.ebs VolumeScanDetails.scanType
service.ebs VolumeScanDetails.sources

Nama bidang JSON
service.event FirstSeen
service.event LastSeen
layanan.malware ScanDetails.scanCategory
layanan.malware ScanDetails.scanConfiguration.incrementalScanDetails.baselineResourceArn
layanan.malware ScanDetails.scanConfiguration.triggerType
layanan.malware ScanDetails.threats.count
layanan.malware ScanDetails.threats.hash
layanan.malware ScanDetails.threats.itemDetails.additionalInfo.deviceName
layanan.malware ScanDetails.threats.itemDetails.additionalInfo.versionId
layanan.malware ScanDetails.threats.itemDetails.hash
layanan.malware ScanDetails.threats.itemDetails.itemPath
layanan.malware ScanDetails.threats.itemDetails.resourceArn
layanan.malware ScanDetails.threats.itemPaths.hash
layanan.malware ScanDetails.threats.itemPaths.nestedItemPath
layanan.malware ScanDetails.threats.source
layanan.malware ScanDetails.uniqueThreatCount
service.runtime Details.context.addressFamily
service.runtime Details.context.commandLineExample
service.runtime Details.context.fileSystemType
service.runtime Details.context.flags

Nama bidang JSON
service.runtime Details.context.ianaProtocolNumber
service.runtime Details.context.ldPreloadValue
service.runtime Details.context.libraryPath
service.runtime Details.context.memoryRegions
service.runtime Details.context.modifiedAt
service.runtime Details.context.modifyingProcess.euid
service.runtime Details.context.modifyingProcess.executablePath
service.runtime Details.context.modifyingProcess.executableSha256
service.runtime Details.context.modifyingProcess.lineage.euid
service.runtime Details.context.modifyingProcess.lineage.executablePath
service.runtime Details.context.modifyingProcess.lineage.name
service.runtime Details.context.modifyingProcess.lineage.namespacePid
service.runtime Details.context.modifyingProcess.lineage.parentUuid
service.runtime Details.context.modifyingProcess.lineage.pid
service.runtime Details.context.modifyingProcess.lineage.startTime
service.runtime Details.context.modifyingProcess.lineage.userId
service.runtime Details.context.modifyingProcess.lineage.uuid
service.runtime Details.context.modifyingProcess.name
service.runtime Details.context.modifyingProcess.namespacePid
service.runtime Details.context.modifyingProcess.parentUuid

Nama bidang JSON
service.runtime Details.context.modifyingProcess.pid
service.runtime Details.context.modifyingProcess.pwd
service.runtime Details.context.modifyingProcess.startTime
service.runtime Details.context.modifyingProcess.user
service.runtime Details.context.modifyingProcess.userId
service.runtime Details.context.modifyingProcess.uuid
service.runtime Details.context.mountSource
service.runtime Details.context.mountTarget
service.runtime Details.context.relatedFilePaths
service.runtime Details.context.releaseAgentPath
service.runtime Details.context.runcBinaryPath
service.runtime Details.context.scriptPath
service.runtime Details.context.serviceName
service.runtime Details.context.shellHistoryFilePath
service.runtime Details.context.socketPath
service.runtime Details.context.targetProcess.euid
service.runtime Details.context.targetProcess.executablePath
service.runtime Details.context.targetProcess.executableSha256
service.runtime Details.context.targetProcess.lineage.euid
service.runtime Details.context.targetProcess.lineage.executablePath

Nama bidang JSON
service.runtime Details.context.targetProcess.lineage.name
service.runtime Details.context.targetProcess.lineage.namespacePid
service.runtime Details.context.targetProcess.lineage.parentUuid
service.runtime Details.context.targetProcess.lineage.pid
service.runtime Details.context.targetProcess.lineage.startTime
service.runtime Details.context.targetProcess.lineage.userId
service.runtime Details.context.targetProcess.lineage.uuid
service.runtime Details.context.targetProcess.name
service.runtime Details.context.targetProcess.namespacePid
service.runtime Details.context.targetProcess.parentUuid
service.runtime Details.context.targetProcess.pid
service.runtime Details.context.targetProcess.pwd
service.runtime Details.context.targetProcess.startTime
service.runtime Details.context.targetProcess.user
service.runtime Details.context.targetProcess.userId
service.runtime Details.context.targetProcess.uuid
service.runtime Details.context.threatFilePath
service.runtime Details.context.toolCategory
service.runtime Details.context.toolName
service.runtime Details.process.euid

Nama bidang JSON
service.runtime Details.process.lineage.euid
service.runtime Details.process.lineage.executablePath
service.runtime Details.process.lineage.name
service.runtime Details.process.lineage.namespacePid
service.runtime Details.process.lineage.parentUuid
service.runtime Details.process.lineage.pid
service.runtime Details.process.lineage.startTime
service.runtime Details.process.lineage.userId
service.runtime Details.process.lineage.uuid
service.runtime Details.process.namespacePid
service.runtime Details.process.parentUuid
service.runtime Details.process.pid
service.runtime Details.process.pwd
service.runtime Details.process.startTime
service.runtime Details.process.user
service.runtime Details.process.userId
service.runtime Details.process.uuid
Service.userFeedback

Aturan penindasan di GuardDuty

Aturan penekanan adalah satu set kriteria, yang terdiri dari atribut filter yang dipasangkan dengan sebuah nilai, digunakan untuk memfilter temuan dengan secara otomatis mengarsipkan temuan baru yang sesuai dengan kriteria yang ditentukan. Aturan penekanan dapat digunakan untuk memfilter temuan bernilai rendah, temuan positif palsu, atau ancaman yang tidak ingin Anda tindaklanjuti, agar lebih mudah mengenali ancaman keamanan dengan dampak paling besar terhadap lingkungan Anda.

Setelah membuat aturan penekanan, temuan baru yang sesuai dengan kriteria yang ditentukan dalam aturan akan diarsipkan secara otomatis selama aturan penekanan berlaku. Anda dapat menggunakan filter yang ada untuk membuat aturan penekanan atau membuat aturan penekanan dari filter baru yang Anda tentukan. Anda dapat mengonfigurasi aturan penekanan untuk menekan seluruh tipe temuan, atau menentukan kriteria filter yang lebih terperinci guna menekan instans spesifik dari tipe temuan tertentu. Anda dapat mengedit aturan penindasan kapan saja.

Temuan yang ditekan tidak dikirim ke AWS Security Hub CSPM, Amazon Simple Storage Service, Amazon Detective, atau Amazon EventBridge, mengurangi tingkat kebisingan pencarian jika Anda menggunakan GuardDuty temuan melalui Security Hub CSPM, SIEM pihak ketiga, atau aplikasi peringatan dan tiket lainnya. Jika Anda telah mengaktifkanPerlindungan Malware untuk EC2, GuardDuty temuan yang ditekan tidak akan memulai pemindaian malware.

GuardDuty terus menghasilkan temuan bahkan ketika mereka cocok dengan aturan penindasan Anda, namun, temuan tersebut secara otomatis ditandai sebagai diarsipkan. Temuan yang diarsipkan disimpan GuardDuty selama 90 hari dan dapat dilihat kapan saja selama periode tersebut. Anda dapat melihat temuan yang ditekan di GuardDuty konsol dengan memilih Diarsipkan dari tabel temuan, atau melalui GuardDuty ListFindings API menggunakan API dengan `findingCriteria` kriteria `service.archived` sama dengan true.

> **Note**
>
> Dalam lingkungan multi-akun hanya GuardDuty administrator yang dapat membuat aturan penindasan.

Menggunakan aturan penindasan dengan Deteksi Ancaman yang Diperluas

GuardDuty Deteksi Ancaman yang Diperluas secara otomatis mendeteksi serangan multi-tahap yang mencakup sumber data, berbagai jenis AWS sumber daya, dan waktu, dalam. Akun AWS

Ini menghubungkan peristiwa di berbagai sumber data untuk mengidentifikasi skenario yang menampilkan dirinya sebagai ancaman potensial terhadap AWS lingkungan Anda, dan kemudian menghasilkan temuan urutan serangan. Untuk informasi selengkapnya, lihat Cara kerja Deteksi Ancaman yang Diperluas.

Saat Anda membuat aturan penindasan yang mengarsipkan temuan, Deteksi Ancaman yang Diperluas tidak dapat menggunakan temuan yang diarsipkan ini saat menghubungkan peristiwa untuk urutan serangan. Aturan penekanan yang luas dapat memengaruhi kemampuan GuardDuty mendeteksi perilaku yang selaras dengan mendeteksi serangan multi-tahap. Temuan yang diarsipkan karena aturan penekanan tidak dianggap sebagai sinyal untuk urutan serangan. Misalnya, jika Anda membuat aturan penindasan yang mengarsipkan semua temuan terkait cluster EKS alih-alih menargetkan aktivitas tertentu yang diketahui, tidak GuardDuty akan dapat menggunakan temuan tersebut untuk mendeteksi urutan serangan di mana aktor ancaman mengeksploitasi wadah, memperoleh token istimewa, dan mengakses sumber daya sensitif.

Pertimbangkan rekomendasi berikut dari GuardDuty:

- Terus gunakan aturan penekanan untuk mengurangi peringatan dari aktivitas tepercaya yang diketahui.
- Jaga agar aturan penindasan tetap fokus pada perilaku tertentu yang tidak GuardDuty ingin Anda hasilkan temuan.

Kasus penggunaan umum untuk aturan penekanan dan contoh

Jenis temuan berikut memiliki kasus penggunaan umum untuk menerapkan aturan penekanan. Pilih nama temuan untuk mempelajari lebih lanjut tentang temuan itu. Tinjau deskripsi kasus penggunaan untuk memutuskan apakah Anda ingin membuat aturan penindasan untuk jenis pencarian tersebut.

> **Important**
>
> GuardDuty merekomendasikan agar Anda membuat aturan penekanan secara reaktif dan hanya untuk temuan yang telah berulang kali Anda identifikasi positif palsu di lingkungan Anda.

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWSGunakan aturan penindasan untuk secara otomatis mengarsipkan temuan yang dihasilkan saat jaringan VPC

dikonfigurasi untuk merutekan lalu lintas internet sedemikian rupa sehingga keluar dari gateway lokal dan bukan dari Gateway Internet VPC.

Temuan ini dibuat saat jaringan dikonfigurasi untuk merutekan lalu lintas internet sedemikian rupa sehingga keluar dari gateway on-premise, bukan dari Gateway Internet VPC (IGW). Konfigurasi umum, seperti penggunaan AWS Outposts, atau koneksi VPN VPC, dapat mengakibatkan lalu lintas dirutekan dengan cara ini. Jika ini adalah perilaku yang diharapkan, disarankan agar Anda menggunakan aturan penekanan dan membuat aturan yang terdiri dari dua kriteria filter. Kriteria pertama adalah tipe temuan, yaitu `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Kriteria filter kedua adalah alamat IPv4 pemanggil API dengan alamat IP atau rentang CIDR dari gateway internet on-premise Anda. Contoh di bawah ini merupakan filter yang akan Anda gunakan untuk menekan tipe temuan ini berdasarkan alamat IP pemanggil API.

```
Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
 API caller IPv4 address: 198.51.100.6
```

> **Note**
>
> Untuk menyertakan beberapa IP pemanggil API, Anda dapat menambahkan setiap alamat IP ke daftar nilai untuk Setara atau NotEquals kondisi, atau menggunakan pola wildcard untuk Kecocokan atau NotMatches kondisi. Nilai Setara atau NotEquals nilai juga dapat berupa rentang CIDR, yang cocok dengan alamat IP apa pun dalam rentang itu.

- Recon:EC2/Portscan – Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis saat menggunakan aplikasi penilaian kerentanan.

  Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `Recon:EC2/Portscan`. Kriteria filter kedua harus sesuai dengan instans atau instans-instans yang menjadi host alat penilaian kerentanan ini. Anda dapat menggunakan atribut ID citra instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang meng-host alat ini. Contoh di bawah ini merupakan filter yang akan Anda gunakan untuk menekan tipe temuan ini berdasarkan instans dengan AMI tertentu.

  ```
  Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
  ```

- UnauthorizedAccess:EC2/SSHBruteForce – Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis ketika ditargetkan ke instans bastion.

Jika target upaya brute force adalah tuan rumah benteng, ini mungkin mewakili perilaku yang diharapkan untuk lingkungan Anda AWS . Jika demikian, kami menyarankan Anda mengatur aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `UnauthorizedAccess:EC2/SSHBruteForce`. Kriteria filter kedua harus sesuai dengan instans atau instans-instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID citra instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang meng-host alat ini. Contoh di bawah ini merupakan filter yang akan Anda gunakan untuk menekan tipe temuan ini berdasarkan instans dengan nilai tanda instans tertentu.

```
Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
```

- Recon:EC2/PortProbeUnprotectedPort – Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis ketika ditargetkan ke instans yang sengaja diekspos.

  Mungkin ada kasus di mana instans sengaja diekspos, misalnya jika instans meng-host server web. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda menyiapkan aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `Recon:EC2/PortProbeUnprotectedPort`. Kriteria filter kedua harus sesuai dengan instans atau instans-instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID citra instans atau atribut nilai Tanda, tergantung kriteria yang dapat diidentifikasi dengan instans yang meng-host alat ini. Contoh di bawah ini merupakan filter yang akan Anda gunakan untuk menekan tipe temuan ini berdasarkan instans dengan kunci tanda instans tertentu di konsol.

  ```
  Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
  ```

Aturan penekanan yang direkomendasikan untuk temuan Pemantauan Runtime

- PrivilegeEscalation:Runtime/DockerSocketAccesseddihasilkan ketika proses di dalam wadah berkomunikasi dengan soket Docker. Mungkin ada wadah di lingkungan Anda yang mungkin perlu mengakses soket Docker untuk alasan yang sah. Akses dari wadah tersebut akan menghasilkan tem PrivilegeEscalation:Runtime/DockerSocketAccessed uan. Jika ini adalah kasus di AWS lingkungan Anda, kami sarankan Anda menyiapkan aturan penindasan untuk jenis temuan ini. Kriteria pertama harus menggunakan bidang Jenis pencarian dengan nilai sama dengan`PrivilegeEscalation:Runtime/DockerSocketAccessed`. Kriteria filter

kedua adalah bidang jalur yang dapat dieksekusi dengan nilai yang sama dengan proses `executablePath` dalam temuan yang dihasilkan. Atau, kriteria filter kedua dapat menggunakan SHA-256 bidang Executable dengan nilai yang sama dengan proses `executableSha256` dalam temuan yang dihasilkan.

- Cluster Kubernetes menjalankan server DNS mereka sendiri sebagai pod, seperti. `coredns` Oleh karena itu, untuk setiap pencarian DNS dari pod, GuardDuty menangkap dua peristiwa DNS — satu dari pod dan yang lainnya dari pod server. Ini dapat menghasilkan duplikat untuk temuan DNS berikut:
  - Backdoor:Runtime/C&CActivity.B! DNS
  - CryptoCurrency:Runtime/BitcoinTool.B! DNS
  - Impact:Runtime/AbusedDomainRequest.Reputation
  - Impact:Runtime/BitcoinDomainRequest.Reputation
  - Impact:Runtime/MaliciousDomainRequest.Reputation
  - Impact:Runtime/SuspiciousDomainRequest.Reputation
  - Trojan:Runtime/BlackholeTraffic! DNS
  - Trojan:Runtime/DGADomainRequest.C! DNS
  - Trojan:Runtime/DriveBySourceTraffic! DNS
  - Trojan:Runtime/DropPoint! DNS
  - Trojan:Runtime/PhishingDomainRequest! DNS

  Temuan duplikat akan mencakup detail pod, container, dan proses yang sesuai dengan pod server DNS Anda. Anda dapat mengatur aturan penindasan untuk menekan temuan duplikat ini menggunakan bidang ini. Kriteria filter pertama harus menggunakan bidang Jenis pencarian dengan nilai yang sama dengan tipe temuan DNS dari daftar temuan yang disediakan sebelumnya di bagian ini. Kriteria filter kedua bisa berupa jalur yang dapat dieksekusi dengan nilai yang sama dengan server DNS Anda `executablePath` atau Executable SHA-256 dengan nilai yang sama dengan server DNS Anda `executableSHA256` dalam temuan yang dihasilkan. Sebagai kriteria filter ketiga opsional, Anda dapat menggunakan bidang gambar kontainer Kubernetes dengan nilai yang sama dengan image wadah dari pod server DNS Anda dalam temuan yang dihasilkan.

Membuat aturan penindasan di GuardDuty

Aturan penindasan adalah sekumpulan kriteria yang mencakup penggunaan atribut filter dan memberikan nilai yang tidak GuardDuty ingin Anda hasilkan jenis temuan. Jenis temuan yang

cocok dengan kriteria ini diarsipkan secara otomatis. Untuk mengurangi kebisingan, temuan yang ditekan tidak dikirim ke salah Layanan AWS satu yang dapat Anda integrasikan. Untuk informasi selengkapnya tentang kasus penggunaan umum untuk membuat aturan penekanan, lihatAturan penekanan.

Anda dapat memvisualisasikan, membuat, dan mengelola aturan penindasan dengan menggunakan halaman aturan penindasan di GuardDuty konsol. Aturan penindasan juga dapat dihasilkan dari filter tersimpan yang ada. Untuk informasi selengkapnya tentang membuat filter, lihatPenyaringan temuan di GuardDuty.

Kriteria filter dapat mencakup kecocokan persis menggunakan E qu als dan NotEquals operator, keco cokan wildcard menggunakan Coco kan dan NotMatches operator atau pen cocokan perbandingan menggunakan GreaterThan, GreaterThanEquals, LessThan dan LessThanEquals operator. Informasi lebih lanjut tentang operator yang tersedia dapat ditemukan di Conditions halaman.

Pilih metode akses pilihan Anda untuk membuat aturan penindasan untuk GuardDuty menemukan jenis.

Console

Untuk membuat aturan penekanan menggunakan konsol:

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Pada halaman aturan penekanan, klik Buat aturan penekanan untuk membuka formulir Buat aturan penekanan.
3. Masukkan Nama untuk aturan penindasan. Nama harus 3-64 karakter. Karakter yang valid adalah a-z, A-Z, 0-9, titik (.), tanda hubung (-), dan garis bawah (_).
4. Des kripsi bersifat opsional. Jika Anda memasukkan deskripsi, itu dapat memiliki hingga 512 karakter. Karakter yang valid adalah a-z, A-Z, 0-9, titik (.), tanda hubung (-), titik dua (:), tanda kurung ({} () []), garis miring maju (/), dan spasi.
5. Per ingkat bersifat opsional. Ini bisa berupa nilai numerik dari 1 hingga jumlah total filter dan aturan penindasan, ditambah 1.
6. Di bawah bagian Atribut, pilih Kunci dan Operator dari drop-down.
7. Masukkan nilai baik “string” atau “tanggal” dari datepicker berdasarkan kunci yang dipilih. Jika itu adalah nilai string, ketik teks dan tekan enter. Beberapa nilai dapat ditambahkan dalam kasus nilai string.

8. Kriteria tambahan dapat ditambahkan dengan memilih Tambahkan Kriteria untuk menambahkan set K unci, Operator, dan Nilai lainnya.
9. Pilih Buat aturan penekanan untuk membuat dan menyimpan aturan penindasan.

Anda juga dapat membuat aturan penekanan dari filter tersimpan yang ada. Untuk informasi selengkapnya tentang membuat filter, lihatPenyaringan temuan di GuardDuty.

Untuk membuat aturan penekanan dari filter tersimpan:

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Pada halaman Temuan, dari menu A turan tersimpan, pilih aturan kumpulan filter yang disimpan. Ini akan secara otomatis menampilkan set filter dan temuan yang sesuai dengan kriteria.
3. Anda juga dapat menambahkan lebih banyak kriteria filter ke aturan yang disimpan ini. Jika Anda tidak memerlukan kriteria filter tambahan, lewati langkah ini. Untuk menambahkan satu atau beberapa kriteria filter, ikuti langkah 3 hingga 7 diAdding filters on Findings page, lalu lanjutkan dengan langkah-langkah berikut.
4. Setelah Anda menambahkan kriteria filter dan mengonfirmasi bahwa temuan yang difilter memenuhi persyaratan Anda, pilih Buat aturan penekanan.
5. Masukkan Nama untuk aturan penindasan. Nama harus 3-64 karakter. Karakter yang valid adalah a-z, A-Z, 0-9, titik (.), tanda hubung (-), dan garis bawah (_).
6. Des kripsi bersifat opsional. Jika Anda memasukkan deskripsi, itu dapat memiliki hingga 512 karakter.
7. Pilih Buat.
8. Jika Anda tidak perlu menambahkan kriteria filter tambahan ke aturan yang disimpan, ikuti langkah 4 hingga 7 untuk membuat filter.

API/CLI

Untuk membuat aturan penekanan menggunakan API:

1. Anda dapat membuat aturan penindasan melalui CreateFilter API. Untuk melakukannya, tentukan kriteria filter dalam file JSON mengikuti format contoh terperinci di bawah ini. Contoh di bawah ini akan menekan temuan tingkat keparahan rendah yang tidak diarsipkan yang memiliki permintaan DNS ke `test.example.com` domain. Untuk temuan tingkat keparahan sedang, daftar input akan menjadi`["4", "5", "7"]`. Untuk temuan tingkat keparahan

tinggi, daftar input akan menjadi`["6", "7", "8"]`. Untuk temuan tingkat keparahan kritis, daftar input akan menjadi`["9", "10"]`. Anda juga dapat memfilter berdasarkan satu nilai dalam daftar.

Contoh berikut menambahkan filter untuk temuan tingkat keparahan rendah untuk fungsi lambda dengan awalan nama fungsi "MyFunc" dan tag fungsi dengan awalan bukan sebagai "" TestTag

```
{
    "Criterion": {
        "service.action.dnsRequestAction.domain": {
            "Equals": [
                "test.example.com"
            ]
        },
        "severity": {
            "Equals": [
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

Anda dapat membuat aturan penindasan menggunakan karakter wildcard * dan? . Karakter pengganti dalam filter didukung hanya menggunakan Co co kan dan NotMatches operator. Untuk mencocokkan sejumlah karakter, Anda dapat menggunakan * dalam nilai atribut dan untuk mencocokkan satu karakter, Anda dapat menggunakan? dalam nilai atribut. Filter mendukung maksimal 5 atribut di bawah satu kondisi wildcard dan maksimal 5 karakter wildcard dalam satu atribut. Contoh berikut menambahkan filter untuk nama Lambda yang cocok dengan awalan “MyFunc" tetapi bukan fungsi Lambda dengan tag dengan "TestTag" sebagai awalan diikuti oleh 0-2 karakter.

```
{
    "Criterion": {
        "resource.lambdaDetails.functionName": {
```

```
            "Matches": [
                "MyFunc*"
            ]
        },
        "resource.lambdaDetails.tags.key": {
            "NotMatches": [
                "TestTag??"
            ]
        }
    }
}
```

Untuk daftar nama bidang JSON dan konsolnya yang setara, lihat Filter properti di GuardDuty.

Untuk menguji kriteria filter Anda, gunakan kriteria JSON yang sama di ListFindings API, dan konfirmasikan bahwa temuan yang benar telah dipilih. Untuk menguji kriteria filter Anda menggunakan AWS CLI ikuti contoh menggunakan file DetectorId dan .json Anda sendiri.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

```
aws guardduty list-detector
```

```
aws guardduty list-findings \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--region us-east-1 \
--finding-criteria file://criteria.json
```

> **Note**
>
> Pencocokan wildcard tidak tersedia untuk ListFindings dan GetFindingsStatistics. Kriteria yang berisi wildcard tidak dapat divalidasi menggunakan ListFindings dan GetFindingsStatistics.

2. Unggah filter Anda untuk digunakan sebagai aturan penekanan dengan CreateFilter API atau dengan menggunakan AWS CLI mengikuti contoh di bawah ini dengan ID detektor Anda sendiri, nama untuk aturan penekanan, dan file.json.

   Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

   ```
   aws guardduty create-filter \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --region us-east-1 \
   --action ARCHIVE \
   --name yourfiltername \
   --finding-criteria file://criteria.json
   ```

Anda dapat melihat daftar filter Anda secara terprogram dengan API. ListFilter Anda dapat melihat detail filter individual dengan memberikan nama filter ke GetFilter API. Perbarui filter menggunakan UpdateFilter atau hapus dengan DeleteFilter API.

Memperbarui aturan penekanan di GuardDuty

Bagian ini menyediakan langkah-langkah untuk memperbarui aturan penindasan di Anda Akun AWS dalam suatu hal tertentu Wilayah AWS.

Anda dapat memperbarui aturan penekanan yang ada dari halaman aturan penekanan di GuardDuty konsol. GuardDuty mendukung pembaruan deskripsi filter penekanan, peringkat dan kriteria filter dari GuardDuty konsol atau dengan menggunakan GuardDuty CLI/API. Memperbarui aturan penekanan mengikuti batasan yang sama pada nilai bidang untuk deskripsi, peringkat, dan kriteria seperti Membuat aturan penekanan.

Jika Anda adalah akun anggota, akun administrator Anda dapat melakukan tindakan ini atas nama Anda. Untuk informasi selengkapnya, lihat Akun administrator dan hubungan akun anggota.

Pilih metode akses pilihan Anda untuk menghapus aturan penindasan untuk GuardDuty findingtypes.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

2. Pada halaman A turan penekanan, pilih aturan penindasan yang akan diperbarui.
3. Dari tarik- turun Tindakan, pilih Per barui aturan penekanan.
4. Ini membuka formulir aturan penindasan yang ada.
5. Buat perubahan pada bagian Deskripsi, Peringkat, dan Atribut sesuai kebutuhan.
6. Pilih Per barui aturan penekanan untuk memperbarui aturan Penindasan.

API/CLI

Untuk memperbarui aturan penekanan menggunakan API:

1. Anda dapat memperbarui aturan penekanan melalui UpdateFilter API. Hanya deskripsi, peringkat, dan kriteria yang dapat diperbarui menggunakan UpdateFilter API. Ketiga bidang ini adalah opsional.
2. Untuk memperbarui filter yang ada, Anda memerlukan nama filter yang Anda rencanakan untuk diperbarui.
3. Jika Anda ingin memperbarui kriteria yang ada, buat file JSON dengan kriteria yang diperbarui mirip dengan cara Anda pertama kali membuat filter. Contoh kriteria untuk menekan temuan tingkat keparahan rendah yang tidak diarsipkan yang memiliki permintaan DNS ke domain test.example.com. Untuk temuan tingkat keparahan sedang, daftar input adalah ["4", “5", “7"]. Untuk temuan tingkat keparahan tinggi, daftar input adalah ["6", “7", “8"]. Untuk temuan tingkat keparahan kritis, daftar input adalah ["9", “10"]. Anda juga dapat memfilter berdasarkan satu nilai dalam daftar. Contoh berikut menambahkan filter untuk temuan tingkat keparahan rendah.

```
{
    "Criterion": {
        "service.action.dnsRequestAction.domain": {
            "Equals": [
                "test.example.com"
            ]
        },
        "severity": {
            "Equals": [
                "1",
                "2",
                "3"
            ]
```

```
        }
    }
}
```

Untuk daftar nama bidang JSON dan konsolnya yang setara, lihat Filter properti di GuardDuty.

Untuk menguji kriteria filter Anda, gunakan kriteria JSON yang sama di ListFindings API, dan konfirmasikan bahwa temuan yang benar telah dipilih. Untuk menguji kriteria filter Anda menggunakan AWS CLI ikuti contoh menggunakan file DetectorId dan .json Anda sendiri.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

```
aws guardduty list-detectors --region us-east-1
```

4. Jika Anda ingin memperbarui deskripsi, Anda dapat menyertakan parameter deskripsi dalam panggilan CLI.
5. Jika Anda ingin memperbarui peringkat, Anda dapat menyertakan parameter peringkat dalam panggilan CLI.
6. Jika Anda ingin memperbarui dari filter penekanan ke filter biasa, gunakan parameter tindakan dan nilai sebagai ARCHIVE dalam panggilan CLI.
7. Perbarui API filter yang ada atau dengan menggunakan contoh AWS CLI berikut di bawah ini dengan ID detektor Anda sendiri, nama untuk aturan penindasan, dan file.json.
8. Berikut ini adalah contoh CLI yang memperbarui semua parameter yang dijelaskan di atas. Anda dapat memilih parameter spesifik yang akan diperbarui untuk kasus penggunaan Anda dari perintah -

```
aws guardduty update-filter \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--region us-east-1 \
--action ARCHIVE \
--rank 1 \
--description "Updated description" \
--finding-criteria file://criteria.json
```

Menghapus aturan penekanan di GuardDuty

Bagian ini menyediakan langkah-langkah untuk menghapus aturan penekanan di Anda Akun AWS di suatu tempat tertentu Wilayah AWS.

Anda mungkin ingin menghapus aturan penindasan yang tidak lagi menggambarkan perilaku yang diharapkan di lingkungan Anda. Anda tidak lagi ingin menekan jenis temuan terkait sehingga GuardDuty dapat menghasilkan tipe pencarian.

Jika Anda adalah akun anggota, akun administrator Anda dapat melakukan tindakan ini atas nama Anda. Untuk informasi selengkapnya, lihat Akun administrator dan hubungan akun anggota.

Pilih metode akses pilihan Anda untuk menghapus aturan penindasan untuk GuardDuty menemukan jenis.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Pada halaman A turan penekanan, pilih aturan penindasan yang akan dihapus.
3. Dari tarik- turun Tindakan, pilih H apus aturan penekanan.
4. Ini meminta pop-up konfirmasi. Pilih Hapus untuk melanjutkan penghapusan. Atau pilih Bat al untuk membatalkan operasi.

API/CLI

Jalankan API DeleteFilter. Tentukan nama filter dan ID detektor terkait untuk Wilayah tertentu.

Atau, Anda dapat menggunakan AWS CLI contoh berikut dengan mengganti nilai yang diformat dalam*red*:

```
aws guardduty delete-filter \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--filter-name filterName \
--region us-east-1
```

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

Metrik aturan penekanan

Dengan Amazon GuardDuty, Anda dapat memantau seberapa sering setiap aturan penekanan cocok dan mengarsipkan temuan. GuardDuty menerbitkan metrik ini ke Amazon CloudWatch di bawah namespace. AWS/GuardDuty

> ⚠ GuardDuty menghitung temuan yang cocok dan menekan temuan secara berbeda
>
> GuardDuty memancarkan FindingsMatchedByFilter ketika temuan cocok dengan aturan penekanan atau filter NOOP (filter tanpa tindakan). Metrik ini meningkat terlepas dari tindakan filter. GuardDuty memancarkan FindingsSuppressedByFilter hanya ketika tindakan aturan adalah Arsip dan aturan adalah aturan pengarsipan prioritas tertinggi untuk temuan itu.

GuardDuty menerbitkan metrik aturan penekanan berdasarkan konfigurasi akun Anda:

- Untuk akun mandiri (bukan bagian dari organisasi), GuardDuty menerbitkan metrik ke akun tersebut.
- Untuk akun yang merupakan bagian dari organisasi, GuardDuty menerbitkan metrik ke akun administrator yang didelegasikan. GuardDuty Untuk informasi selengkapnya tentang cara kerja akun administrator dan anggota GuardDuty, lihatMengelola banyak akun di Amazon GuardDuty.

Detail metrik

Tabel berikut menjelaskan CloudWatch metrik Amazon yang GuardDuty diterbitkan untuk aturan penekanan.

Metrik	Unit	Deskripsi
`FindingsMatchedByFilter`	Hitungan	Jumlah temuan yang cocok dengan kriteria aturan penekanan atau filter NOOP.

Metrik	Unit	Deskripsi
		Temuan dapat mencocokkan beberapa aturan penekanan atau filter NOOP, dan GuardDuty menghitun gnya sekali per pertandin gan. Setiap pertandingan menghasilkan 1 titik data.
`FindingsSuppressed ByFilter`	Hitungan	Jumlah temuan yang diarsipka n oleh aturan penindasan. Ketika beberapa aturan cocok dengan temuan yang sama, hanya GuardDuty menghitun g aturan dengan `Rank` nilai terendah. Setiap penekanan menghasilkan 1 titik data.

Lihat metrik aturan penekanan di Amazon CloudWatch

Anda dapat menemukan metrik aturan penekanan di CloudWatch konsol Amazon di bawah AWS/GuardDutynamespace, yang dikelompokkan berdasarkan dimensi. FilterName Nilai `FilterName` dimensi adalah nama aturan penekanan atau filter. Untuk petunjuk tentang menemukan dan membuat grafik metrik di Amazon CloudWatch, lihat Melihat metrik yang tersedia di Panduan Pengguna Amazon. CloudWatch

Menyesuaikan deteksi ancaman dengan daftar entitas dan daftar alamat IP

Amazon GuardDuty memantau keamanan AWS lingkungan Anda dengan menganalisis dan memproses Log Aliran VPC, log AWS CloudTrail peristiwa, dan log DNS. Dengan mengaktifkan satu atau lebih rencana GuardDuty perlindungan Use-case terfokus (kecualiPemantauan Runtime), Anda dapat memperluas kemampuan pemantauan di dalamnya GuardDuty.

Dengan daftar, GuardDuty membantu Anda menyesuaikan ruang lingkup deteksi ancaman di lingkungan Anda. Anda dapat mengonfigurasi GuardDuty untuk berhenti menghasilkan temuan

dari sumber tepercaya Anda dan menghasilkan temuan untuk sumber berbahaya yang diketahui dari daftar ancaman Anda. GuardDuty terus mendukung daftar alamat IP lama dan memperluas dukungan ke daftar entitas (disarankan) yang dapat berisi alamat IP, domain, atau keduanya.

Topik

- Memahami daftar entitas dan daftar alamat IP
- Pertimbangan penting untuk daftar GuardDuty
- Format daftar
- Memahami status daftar
- Menyiapkan prasyarat untuk daftar entitas dan daftar alamat IP
- Menambahkan dan mengaktifkan daftar entitas atau daftar IP
- Memperbarui daftar entitas atau daftar alamat IP
- De-activating daftar entitas atau daftar alamat IP
- Menghapus daftar entitas atau daftar alamat IP

Memahami daftar entitas dan daftar alamat IP

GuardDuty menawarkan dua pendekatan implementasi: daftar entitas (direkomendasikan) dan daftar IP. Kedua pendekatan membantu Anda menentukan sumber tepercaya, yang berhenti GuardDuty dari menghasilkan temuan dan ancaman yang diketahui, yang GuardDuty digunakan untuk menghasilkan temuan.

Daftar entitas mendukung alamat IP, nama domain, dan hash SHA-256 file. Mereka menggunakan akses langsung Amazon Simple Storage Service (Amazon S3) dengan izin IAM tunggal yang tidak memengaruhi batas ukuran kebijakan IAM di beberapa Wilayah.

Daftar IP hanya mendukung alamat IP dan penggunaan GuardDuty peran terkait layanan (SLR) (SLR), yang memerlukan pembaruan kebijakan IAM per Wilayah, yang dapat memengaruhi batas ukuran kebijakan IAM.

Daftar tepercaya (baik daftar entitas maupun daftar alamat IP) menyertakan entri yang Anda percayai untuk komunikasi aman dengan AWS infrastruktur Anda. GuardDuty tidak menghasilkan temuan untuk entri yang tercantum dalam sumber tepercaya. Pada waktu tertentu, Anda hanya dapat menambahkan satu daftar entitas tepercaya dan satu daftar alamat IP tepercaya Akun AWS per Wilayah.

Daftar ancaman (baik daftar entitas dan daftar alamat IP) termasuk entri yang telah Anda identifikasi sebagai sumber berbahaya yang dikenal. Ketika GuardDuty mendeteksi aktivitas yang melibatkan sumber-sumber ini, itu menghasilkan temuan untuk mengingatkan Anda tentang potensi masalah keamanan. Anda dapat membuat daftar ancaman Anda sendiri atau memasukkan umpan intelijen ancaman pihak ketiga. Daftar ini dapat disediakan oleh intelijen ancaman pihak ketiga atau dibuat khusus untuk organisasi Anda. Selain menghasilkan temuan karena aktivitas yang berpotensi mencurigakan, GuardDuty juga menghasilkan temuan berdasarkan aktivitas yang melibatkan entri dari daftar ancaman Anda. Pada waktu tertentu, Anda dapat mengunggah hingga enam daftar entitas ancaman dan daftar alamat IP ancaman Akun AWS per Wilayah.

> **Note**
>
> Untuk bermigrasi dari daftar alamat IP ke daftar entitas, ikutiPrasyarat untuk daftar entitas, lalu tambahkan dan aktifkan daftar entitas yang diperlukan. Setelah ini, Anda dapat memilih untuk menonaktifkan atau menghapus daftar alamat IP yang sesuai.

Pertimbangan penting untuk daftar GuardDuty

Sebelum Anda mulai bekerja dengan daftar, baca pertimbangan berikut:

- Daftar alamat IP dan daftar entitas hanya berlaku untuk lalu lintas yang ditujukan untuk alamat IP dan domain yang dapat dirutekan secara publik.
- Dalam daftar entitas, entri berlaku untuk, Log Aliran VPC di Amazon VPC CloudTrail, dan temuan log kueri DNS Route53 Resolver.

  Dalam daftar alamat IP, entri berlaku untuk CloudTrail dan Log Aliran VPC di temuan Amazon VPC, tetapi tidak untuk temuan log kueri DNS Route53 Resolver.
- Jika Anda menyertakan alamat IP atau domain yang sama dalam daftar tepercaya dan ancaman, maka entri ini dalam daftar tepercaya akan diutamakan. GuardDuty tidak akan menghasilkan temuan jika ada aktivitas yang terkait dengan entri ini.
- Dalam lingkungan multi-akun, hanya akun GuardDuty administrator yang dapat mengelola daftar. Pengaturan ini secara otomatis berlaku untuk akun anggota. GuardDuty menghasilkan temuan berdasarkan aktivitas yang melibatkan alamat IP berbahaya yang diketahui (dan domain) dari sumber ancaman akun administrator, dan tidak menghasilkan temuan berdasarkan aktivitas yang melibatkan alamat IP (dan domain) dari sumber tepercaya akun administrator. Untuk informasi selengkapnya, lihat Mengelola banyak akun di Amazon GuardDuty.

- Hanya alamat IPv4 yang diterima. Alamat IPv6 tidak didukung.
- SHA-256 hash file hanya didukung dalam daftar entitas ancaman. Anda tidak dapat menyertakan hash file dalam daftar entitas tepercaya atau daftar alamat IP.
- Setelah Anda mengaktifkan, menonaktifkan, atau menghapus daftar entitas atau daftar alamat IP, proses diperkirakan selesai dalam waktu 15 menit. Dalam skenario tertentu, mungkin diperlukan waktu hingga 40 menit untuk menyelesaikan proses ini.
- GuardDuty menggunakan daftar untuk deteksi ancaman hanya ketika status daftar menjadi Aktif.
- Setiap kali Anda menambahkan atau memperbarui entri di lokasi bucket S3 daftar, Anda harus mengaktifkan daftar lagi. Untuk informasi selengkapnya, lihat Memperbarui daftar entitas atau daftar alamat IP.
- Daftar entitas dan alamat IP memiliki kuota yang berbeda. Untuk informasi selengkapnya, lihat GuardDuty kuota.

Format daftar

GuardDuty menerima beberapa format file untuk daftar dan daftar entitas Anda, dengan maksimum 35 MB per file. Setiap format memiliki persyaratan dan kemampuan khusus.

Plaintext (TXT)

Format ini mendukung alamat IP, rentang CIDR, nama domain, dan hash SHA-256 file. SHA-256 hash file hanya didukung dalam daftar entitas ancaman. Setiap entri harus muncul pada baris terpisah.

Example Contoh untuk daftar entitas

```
192.0.2.1
192.0.2.0/24
example.com
example.org
*.example.org
```

Example Contoh untuk daftar entitas ancaman dengan hash file

```
192.0.2.1
192.0.2.0/24
example.com
example.org
```

```
*.example.org
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3
```

Example Contoh untuk daftar alamat IP

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

Ekspresi Informasi Ancaman Terstruktur (STIX)

Format ini mendukung alamat IP, blok CIDR, nama domain, dan hash SHA-256 file. STIX memungkinkan Anda untuk memasukkan konteks tambahan dengan intelijen ancaman Anda. GuardDuty memproses alamat IP, rentang CIDR, nama domain, dan hash SHA-256 file dari indikator STIX. SHA-256 hash file hanya didukung dalam daftar entitas ancaman.

Example Contoh untuk daftar entitas

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
    id="example:Package-a1b2c3d4-1111-2222-3333-444455556666"
    version="1.2">
    <stix:Indicators>
        <stix:Indicator
            id="example:indicator-a1b2c3d4-aaaa-bbbb-cccc-ddddeeeeffff"
            timestamp="2025-08-12T00:00:00Z"
            xsi:type="indicator:IndicatorType"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <indicator:Title>Malicious domain observed Example</indicator:Title>
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
 Watchlist</indicator:Type>
            <indicator:Observable id="example:Observable-0000-1111-2222-3333">
                <cybox:Object id="example:Object-0000-1111-2222-3333">
                    <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType">
```

```
                        <DomainNameObj:Value condition="Equals">bad.example.com</
DomainNameObj:Value>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

Example Contoh untuk daftar entitas ancaman dengan hash file

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
    xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
    id="example:Package-a1b2c3d4-1111-2222-3333-444455556666"
    version="1.2">
    <stix:Indicators>
        <stix:Indicator
            id="example:indicator-a1b2c3d4-aaaa-bbbb-cccc-ddddeeeeffff"
            timestamp="2025-08-12T00:00:00Z"
            xsi:type="indicator:IndicatorType"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <indicator:Title>Malicious domain observed Example</indicator:Title>
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
 Watchlist</indicator:Type>
            <indicator:Observable id="example:Observable-0000-1111-2222-3333">
                <cybox:Object id="example:Object-0000-1111-2222-3333">
                    <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType">
                        <DomainNameObj:Value condition="Equals">bad.example.com</
DomainNameObj:Value>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
        <stix:Indicator
```

```
            id="example:indicator-a1b2c3d4-eeee-ffff-0000-111122223333"
            timestamp="2025-08-12T00:00:00Z"
            xsi:type="indicator:IndicatorType"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <indicator:Title>File hash for malware variant</indicator:Title>
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">File Hash
 Watchlist</indicator:Type>
            <indicator:Observable id="example:Observable-4444-5555-6666-7777">
                <cybox:Object id="example:File-4444-5555-6666-7777">
                    <cybox:Properties xsi:type="FileObj:FileObjectType">
                        <FileObj:Hashes>
                            <cyboxCommon:Hash>
                                <cyboxCommon:Type
 xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256</cyboxCommon:Type>
                                <cyboxCommon:Simple_Hash_Value
 condition="Equals">a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3</
cyboxCommon:Simple_Hash_Value>
                            </cyboxCommon:Hash>
                        </FileObj:Hashes>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

Example Contoh untuk daftar alamat IP

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
```

```
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
    id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
    version="1.2">
    <stix:Observables cybox_major_version="1" cybox_minor_version="1">
        <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
            <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">

 <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
            <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable
 id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
            <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
```

```
</stix:STIX_Package>
```

Buka Pertukaran Ancaman (OTX) TM CSV

Format ini mendukung blok CIDR, alamat IP individual, domain, dan jenis SHA256 indikator untuk hash file. SHA-256 hash file hanya didukung dalam daftar entitas ancaman. Format file ini memiliki nilai yang dipisahkan koma.

Example Contoh untuk daftar entitas

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
Domain name, example.net, example
```

Example Contoh untuk daftar entitas ancaman dengan hash file

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
Domain name, example.net, example
SHA256, a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3, example
```

Example Contoh untuk daftar alamat IP

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

FireEyeCSV Intelijen Ancaman TM iSight

Format ini mendukung blok CIDR, alamat IP individual, domain, dan hash SHA-256 file di kolom. `sha256` SHA-256 hash file hanya didukung dalam daftar entitas ancaman. Daftar contoh berikut menggunakan format `FireEye`TM CSV.

Example Contoh untuk daftar entitas

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
```

```
 recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,
 sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,
 filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,
 protocol, registrantEmail, registrantName, networkType, url, malwareFamily,
 malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , ,
```

```
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400

 01-00000002, Malicious domain observed in test, Test, Operational, threat,
 1494944400, https://www.example.com/report/01-00000002,https://www.example.com/
report/01-00000002,,,,,,,,,,,,,,,,,,,,,,,, 203.0.113.0/24, example.com,, Related,
 203.0.113.0, 8080, UDP,,, network,, Ursnif, fc13984c-c767-40c9-8329-f4c59557f73b,,,
 1494944400

01-00000005, Malicious file hash, Test, Operational, threat,
 1494944400, https://www.example.com/report/01-00000005, https://
www.example.com/report/01-00000005, , , , , , , , , , , , , , , ,
 a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3, , , , , , , , , , , ,
 Related, , , , , , network, , Ursnif, 9b9a6ea0-3cbf-4e12-bd3e-0c1d7b4e5f6a, , ,
 1494944400
```

Example Contoh untuk daftar alamat IP

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
 recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,
 sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,
 filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,
 protocol, registrantEmail, registrantName, networkType, url, malwareFamily,
 malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400
```

```
01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

Bukti TM ET Intelijen Umpan CSV

Dalam format ProofPoint CSV, Anda dapat menambahkan IP baik alamat atau nama domain dalam satu daftar. Daftar contoh berikut menggunakan format `Proofpoint` CSV. Memberikan nilai untuk `ports` parameter adalah opsional. Ketika Anda tidak menyediakannya, tinggalkan tanda koma (,) di bagian akhir.

Example Contoh untuk daftar entitas

```
domain, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

Example Contoh untuk daftar alamat IP

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

AlienVaultUmpan Reputasi TM

Daftar contoh berikut menggunakan `AlienVault` format. Format ini juga mendukung hash SHA-256 file di kolom indikator. SHA-256 hash file hanya didukung dalam daftar entitas ancaman.

Example Contoh untuk daftar entitas

```
192.0.2.1#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
192.0.2.2#4#2#Scanning Host#IN#Gurgaon#28.4666996002,77.0333023071#3
```

```
192.0.2.3#4#2##CN#Guangzhou#23.1166992188,113.25#3
www.test.org#4#2#Malicious Host#CA#Brossard#45.4673995972,-73.4832000732#3
www.example.com#4#2#Malicious Host#PL##52.2393989563,21.0361995697#3
```

Example Contoh untuk daftar entitas ancaman dengan hash file

```
192.0.2.1#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
192.0.2.2#4#2#Scanning Host#IN#Gurgaon#28.4666996002,77.0333023071#3
192.0.2.3#4#2##CN#Guangzhou#23.1166992188,113.25#3
www.test.org#4#2#Malicious Host#CA#Brossard#45.4673995972,-73.4832000732#3
www.example.com#4#2#Malicious Host#PL##52.2393989563,21.0361995697#3
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3#4#2#Malicious
 Hash###0.0,0.0#3
```

Example Contoh untuk daftar alamat IP

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

Memahami status daftar

Saat Anda menambahkan daftar entitas atau daftar alamat IP, GuardDuty menampilkan status daftar tersebut. Kolom Status menunjukkan apakah daftar efektif dan jika ada tindakan yang diperlukan. Daftar berikut menjelaskan nilai status yang valid:

- Aktif - Menunjukkan daftar sedang digunakan untuk deteksi ancaman kustom.
- Tidak aktif - Menunjukkan bahwa daftar saat ini tidak digunakan. GuardDuty Untuk menggunakan daftar ini untuk deteksi ancaman di lingkungan Anda, lihat Langkah 3: Mengaktifkan daftar entitas atau daftar alamat IP di[Menambahkan dan mengaktifkan daftar entitas atau daftar IP](#).
- Kesalahan - Menunjukkan bahwa ada masalah dengan daftar. Arahkan kursor ke status untuk melihat detail kesalahan.
- Mengaktifkan — Menunjukkan bahwa GuardDuty telah memulai proses mengaktifkan daftar. Anda dapat terus memantau status untuk daftar ini. Jika tidak ada kesalahan, status harus diperbarui ke Aktif. Meskipun status tetap Aktif, Anda tidak dapat melakukan tindakan apa pun di daftar ini. Mungkin perlu beberapa menit agar status daftar berubah menjadi Aktif.
- Menonaktifkan - Menunjukkan bahwa GuardDuty telah memulai proses menonaktifkan daftar. Anda dapat terus memantau status untuk daftar ini. Jika tidak ada kesalahan, status harus diperbarui ke

Tidak Aktif. Meskipun status tetap Menonaktifkan, Anda tidak dapat melakukan tindakan apa pun di daftar ini.

- Hapus Tertunda — Menunjukkan bahwa daftar sedang dalam proses dihapus. Meskipun status tetap Hapus Tertunda, Anda tidak dapat melakukan tindakan apa pun di daftar ini.

Menyiapkan prasyarat untuk daftar entitas dan daftar alamat IP

GuardDuty menggunakan daftar entitas dan daftar alamat IP untuk menyesuaikan deteksi ancaman di AWS lingkungan Anda. Daftar entitas (disarankan) mendukung alamat IP dan nama domain, sedangkan daftar alamat IP hanya mendukung alamat IP. Sebelum Anda mulai membuat daftar ini, Anda harus menambahkan izin yang diperlukan untuk jenis daftar yang ingin Anda gunakan.

Prasyarat untuk daftar entitas

Saat Anda menambahkan daftar entitas, GuardDuty baca daftar intelijen tepercaya dan ancaman Anda dari bucket S3. Peran yang Anda gunakan untuk membuat daftar entitas harus memiliki `s3:GetObject` izin untuk bucket S3 berisi daftar ini.

> **Note**
>
> Dalam lingkungan multi-akun, hanya akun GuardDuty administrator yang dapat mengelola daftar, yang secara otomatis berlaku untuk akun anggota.

Jika Anda belum memiliki `s3:GetObject` izin untuk lokasi bucket S3, gunakan contoh kebijakan berikut dan ganti *`amzn-s3-demo-bucket`* dengan lokasi bucket S3 Anda.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[object-key]"
        }
    ]
```

```
}
```

Prasyarat untuk daftar alamat IP

Berbagai identitas IAM memerlukan izin khusus untuk bekerja dengan daftar IP tepercaya dan daftar ancaman. GuardDuty Identitas dengan kebijakan AmazonGuardDutyFullAccess_v2 (disarankan) terkelola terlampir hanya dapat mengganti nama dan menonaktifkan daftar IP tepercaya yang diunggah dan daftar ancaman.

Untuk memberikan berbagai identitas akses penuh untuk bekerja dengan daftar IP tepercaya dan daftar ancaman (selain mengganti nama dan menonaktifkan, ini termasuk menambahkan, mengaktifkan, menghapus, dan memperbarui lokasi atau nama daftar), pastikan bahwa tindakan berikut ada dalam kebijakan izin yang dilampirkan ke pengguna, grup, atau peran:

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> Tindakan ini tidak termasuk dalam kebijakan yang `AmazonGuardDutyFullAccess` dikelola.

Menggunakan SSE-KMS enkripsi dengan daftar entitas dan daftar IP

GuardDuty dukungan SSE-AES256 dan SSE-KMS enkripsi untuk daftar Anda. SSE-C tidak didukung. Untuk informasi selengkapnya tentang jenis enkripsi untuk S3, lihat Melindungi data menggunakan enkripsi sisi server.

Terlepas dari apakah Anda menggunakan daftar entitas atau daftar IP, jika Anda menggunakan SSE-KMS, tambahkan pernyataan berikut ke AWS KMS key kebijakan Anda. Ganti *123456789012* dengan ID akun Anda sendiri.

```
{
```

```
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

Menambahkan dan mengaktifkan daftar entitas atau daftar IP

Daftar entitas dan daftar alamat IP membantu Anda menyesuaikan kemampuan deteksi ancaman di GuardDuty. Untuk informasi lebih lanjut tentang daftar ini, lihatMemahami daftar entitas dan daftar alamat IP. Untuk mengelola data intelijen tepercaya dan ancaman untuk AWS lingkungan Anda, sar GuardDuty ankan menggunakan daftar entitas. Sebelum Anda memulai, lihat Menyiapkan prasyarat untuk daftar entitas dan daftar alamat IP.

Pilih salah satu metode akses berikut untuk menambahkan dan mengaktifkan daftar entitas tepercaya, daftar entitas ancaman, daftar IP tepercaya, atau daftar IP ancaman.

Console

(Opsional) langkah 1: Mengambil URL lokasi daftar Anda

1. Buka konsol Amazon S3 di https://console.aws.amazon.com/s3/.
2. Di panel navigasi, pilih Bucket.
3. Pilih nama bucket Amazon S3 yang berisi daftar spesifik yang ingin Anda tambahkan.
4. Pilih nama objek (daftar) untuk melihat detailnya.
5. Di bawah tab Properties, salin URI S3 untuk objek ini.

Langkah 2: Menambahkan data intelijen tepercaya atau ancaman

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Daftar, pilih tab Daftar entitas atau Daftar alamat IP.
4. Berdasarkan tab yang Anda pilih, pilih untuk menambahkan daftar tepercaya atau daftar ancaman.

5. Di kotak dialog untuk menambahkan daftar tepercaya atau ancaman, lakukan langkah-langkah berikut:

   a. Untuk Nama daftar, masukkan nama untuk daftar Anda.

      Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).

      Untuk daftar alamat IP, nama daftar Anda harus unik dalam Akun AWS dan Wilayah.

   b. Untuk Lokasi, berikan lokasi tempat Anda mengunggah daftar Anda. Jika Anda belum memilikinya, lihatStep 1: Fetching location URL of your list.

      Hanya berlaku untuk ancaman kustom dan kumpulan entitas tepercaya kustom — Jika Anda memberikan URL lokasi yang tidak cocok dengan format yang didukung berikut, maka Anda akan menerima pesan galat selama penambahan daftar dan aktivasi.

      Format URL lokasi:

      - https://s3.amazonaws.com/bucket.name/file.txt
      - https://s3-aws-region.amazonaws.com/bucket.name/file.txt
      - http://bucket.s3.amazonaws.com/file.txt
      - http://bucket.s3-aws-region.amazonaws.com/file.txt
      - s3://bucket. name/file.txt

   c. (Opsional) Untuk pemilik bucket yang diharapkan, Anda dapat memasukkan Akun AWS ID yang memiliki bucket Amazon S3 yang ditentukan di bidang Lokasi.

      Bila Anda tidak menentukan pemilik Akun AWS ID, maka GuardDuty berperilaku berbeda untuk daftar entitas dan daftar alamat IP. Untuk daftar entitas, GuardDuty akan memvalidasi bahwa akun anggota saat ini memiliki bucket S3 yang ditentukan di bidang Lokasi. Untuk daftar alamat IP, jika Anda tidak menentukan pemilik Akun AWS ID, GuardDuty tidak melakukan validasi apa pun.

      Jika GuardDuty menemukan bahwa bucket S3 ini bukan milik ID akun yang ditentukan, Anda akan mendapatkan kesalahan pada saat mengaktifkan daftar.

   d. Pilih kotak centang Saya setuju.

   e. Pilih Tambah daftar. Secara default, Status daftar yang ditambahkan adalah Tidak aktif. Agar daftar menjadi efektif, Anda harus mengaktifkan daftar.

Langkah 3: Mengaktifkan daftar entitas atau daftar alamat IP

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Daftar, pilih tab di mana Anda ingin mengaktifkan daftar - Daftar entitas atau daftar alamat IP.
4. Pilih satu daftar yang ingin Anda aktifkan. Ini akan mengaktifkan menu Action dan Edit.
5. Pilih T ind akan, lalu pilih Aktifkan.

API/CLI

Untuk menambahkan dan mengaktifkan daftar entitas tepercaya

1. Jalankan CreateTrustedEntitySet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda buat daftar entitas tepercaya ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

   Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).
2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut:

```
aws guardduty create-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganizationListEXAMPLE" \
--format TXT \
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
--activate
```

   Ganti `detector-id` dengan ID detektor akun anggota yang akan Anda buat daftar entitas tepercaya, dan nilai placeholder lainnya. *shown in red*

   Jika Anda tidak ingin mengaktifkan daftar yang baru dibuat ini, maka ganti parameter `--activate` dengan`--no-activate`.

Parameter `expected-bucket-owner` bersifat opsional. Apakah Anda menentukan nilai untuk parameter ini atau tidak, GuardDuty memvalidasi bahwa Akun AWS ID yang terkait dengan `--detector-id` nilai ini memiliki bucket S3 yang ditentukan dalam `--location` parameter. Jika GuardDuty menemukan bahwa bucket S3 ini bukan milik ID akun yang ditentukan, Anda akan mendapatkan kesalahan pada saat mengaktifkan daftar ini.

Hanya berlaku untuk ancaman kustom dan kumpulan entitas tepercaya kustom — Jika Anda memberikan URL lokasi yang tidak cocok dengan format yang didukung berikut, maka Anda akan menerima pesan galat selama penambahan daftar dan aktivasi.

Untuk menambahkan dan mengaktifkan daftar entitas ancaman

1. Jalankan CreateThreatEntitySet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda buat daftar entitas ancaman ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

   Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).

2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut:

   ```
   aws guardduty create-threat-entity-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganizationListEXAMPLE" \
   --format TXT \
   --location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
   --activate
   ```

   Ganti `detector-id` dengan ID detektor akun anggota yang akan Anda buat daftar entitas tepercaya, dan nilai placeholder lainnya. *shown in red*

   Jika Anda tidak ingin mengaktifkan daftar yang baru dibuat ini, maka ganti parameter `--activate` dengan`--no-activate`.

   Parameter `expected-bucket-owner` bersifat opsional. Apakah Anda menentukan nilai untuk parameter ini atau tidak, GuardDuty memvalidasi bahwa Akun AWS ID yang terkait

dengan `--detector-id` nilai ini memiliki bucket S3 yang ditentukan dalam `--location` parameter. Jika GuardDuty menemukan bahwa bucket S3 ini bukan milik ID akun yang ditentukan, Anda akan mendapatkan kesalahan pada saat mengaktifkan daftar ini.

Hanya berlaku untuk ancaman kustom dan kumpulan entitas tepercaya kustom — Jika Anda memberikan URL lokasi yang tidak cocok dengan format yang didukung berikut, maka Anda akan menerima pesan galat selama penambahan daftar dan aktivasi.

Untuk menambah dan mengaktifkan daftar alamat IP tepercaya

1. Jalankan CreateIPset. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda buat daftar alamat IP tepercaya ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

   Untuk daftar alamat IP, nama daftar Anda harus unik dalam Akun AWS dan Wilayah.

   Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).

2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut dan pastikan untuk menggantinya `detector-id` dengan ID detektor akun anggota yang akan Anda perbarui daftar alamat IP tepercaya.

   ```
   aws guardduty create-ip-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganizationListEXAMPLE" \
   --format TXT \
   --location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
   --activate
   ```

   Ganti `detector-id` dengan ID detektor akun anggota yang akan Anda buat daftar IP tepercaya, dan nilai placeholder lainnya. *shown in red*

   Jika Anda tidak ingin mengaktifkan daftar yang baru dibuat ini, maka ganti parameter `--activate` dengan`--no-activate`.

   Parameter `expected-bucket-owner` bersifat opsional. Bila Anda tidak menentukan ID akun yang memiliki bucket S3, GuardDuty tidak akan melakukan validasi apa pun. Saat Anda

menentukan ID akun untuk `expected-bucket-owner` parameter, GuardDuty memvalidasi bahwa Akun AWS ID ini memiliki bucket S3 yang ditentukan dalam `--location` parameter. Jika GuardDuty menemukan bahwa bucket S3 ini bukan milik ID akun yang ditentukan, Anda akan mendapatkan kesalahan pada saat mengaktifkan daftar ini.

Untuk menambah dan mengaktifkan daftar IP ancaman

1. Jalankan CreateThreatIntelSet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda buat daftar alamat IP ancaman ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

   Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).

   Untuk daftar alamat IP, nama daftar Anda harus unik dalam Akun AWS dan Wilayah.

2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut dan pastikan untuk menggant `detector-id` inya dengan ID detektor akun anggota yang akan Anda perbarui daftar IP ancaman.

   ```
   aws guardduty create-threat-intel-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganizationListEXAMPLE" \
   --format TXT \
   --location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
   --activate
   ```

   Ganti `detector-id` dengan ID detektor akun anggota tempat Anda akan membuat daftar IP ancaman, dan nilai placeholder lainnya. *`shown in red`*

   Jika Anda tidak ingin mengaktifkan daftar yang baru dibuat ini, maka ganti parameter `--activate` dengan`--no-activate`.

   Parameter `expected-bucket-owner` bersifat opsional. Bila Anda tidak menentukan ID akun yang memiliki bucket S3, GuardDuty tidak akan melakukan validasi apa pun. Saat Anda menentukan ID akun untuk `expected-bucket-owner` parameter, GuardDuty memvalidasi bahwa Akun AWS ID ini memiliki bucket S3 yang ditentukan dalam `--location` parameter.

Jika GuardDuty menemukan bahwa bucket S3 ini bukan milik ID akun yang ditentukan, Anda akan mendapatkan kesalahan pada saat mengaktifkan daftar ini.

Setelah Anda mengaktifkan daftar entitas atau daftar alamat IP, mungkin perlu beberapa menit agar daftar ini efektif. Lihat informasi yang lebih lengkap di Pertimbangan penting untuk daftar GuardDuty.

Memperbarui daftar entitas atau daftar alamat IP

Daftar entitas dan daftar alamat IP membantu Anda menyesuaikan kemampuan deteksi ancaman GuardDuty. Untuk informasi selengkapnya tentang daftar ini, lihatMemahami daftar entitas dan daftar alamat IP.

Anda dapat memperbarui nama daftar, lokasi bucket S3, ID akun pemilik bucket yang diharapkan, dan entri dalam daftar yang ada. Jika Anda memperbarui entri dalam daftar, Anda harus mengikuti langkah-langkah untuk mengaktifkan daftar lagi GuardDuty untuk menggunakan versi terbaru dari daftar. Setelah Anda memperbarui atau mengaktifkan daftar entitas atau daftar alamat IP, mungkin perlu beberapa menit agar daftar ini efektif. Untuk informasi selengkapnya, lihat Pertimbangan penting untuk daftar GuardDuty.

> **Note**
>
> Jika status daftar adalah Mengaktifkan, Menonaktifkan, atau Menghapus Pending, Anda harus menunggu beberapa menit sebelum melakukan tindakan apa pun. Untuk informasi tentang status ini, lihatMemahami status daftar.

Pilih salah satu metode akses untuk memperbarui daftar entitas atau daftar alamat IP.

Console

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Daftar, pilih tab yang sesuai - Daftar entitas atau daftar alamat IP.
4. Pilih satu daftar (tepercaya atau ancaman) yang ingin Anda perbarui. Ini akan mengaktifkan menu Action and Edit.
5. Pilih Edit.
6. Di kotak dialog untuk memperbarui daftar, tentukan detail yang ingin Anda perbarui.

Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).

Untuk daftar alamat IP, nama daftar Anda harus unik di dalam Akun AWS dan Wilayah.

Hanya berlaku untuk ancaman kustom dan kumpulan entitas tepercaya kustom — Jika Anda memberikan URL lokasi yang tidak cocok dengan format yang didukung berikut, maka Anda akan menerima pesan galat selama penambahan daftar dan aktivasi.

7. (Opsional) Untuk pemilik bucket yang Diharapkan, Anda dapat memasukkan Akun AWS ID yang memiliki bucket Amazon S3 yang ditentukan di bidang Lokasi.

   Bila Anda tidak menentukan pemilik Akun AWS ID, maka GuardDuty berperilaku berbeda untuk daftar entitas dan daftar alamat IP. Untuk daftar entitas, GuardDuty akan memvalidasi bahwa akun anggota saat ini memiliki bucket S3 yang ditentukan di bidang Lokasi. Untuk daftar alamat IP, jika Anda tidak menentukan pemilik Akun AWS ID, GuardDuty tidak akan melakukan validasi apa pun.

   Jika GuardDuty menemukan bahwa bucket S3 ini bukan milik ID akun yang ditentukan, Anda akan mendapatkan kesalahan pada saat mengaktifkan daftar.
8. Pilih kotak centang Saya setuju, lalu pilih Perbarui daftar.

API/CLI

Untuk memulai dengan prosedur berikut, Anda memerlukan ID, seperti,`trustedEntitySetId`,`threatEntitySetId`, atau `trustedIpSetthreatIpSet`, yang terkait dengan sumber daya daftar yang ingin Anda perbarui.

Untuk memperbarui dan mengaktifkan daftar entitas tepercaya

1. Jalankan UpdateTrustedEntitySet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda perbarui daftar entitas tepercaya ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

   Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).
2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut yang `name` memperbarui daftar dan juga mengaktifkan daftar ini:

```
aws guardduty update-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \
--activate
```

Ganti `detector-id` dengan ID detektor akun anggota tempat Anda akan membuat daftar entitas tepercaya, dan nilai placeholder lainnya. *shown in red*

Jika Anda tidak ingin mengaktifkan daftar yang baru dibuat ini, ganti parameternya `--activate` dengan`--no-activate`.

Parameter `expected-bucket-owner` bersifat opsional. Apakah Anda menentukan nilai untuk parameter ini atau tidak, GuardDuty memvalidasi bahwa Akun AWS ID yang terkait dengan `--detector-id` nilai ini memiliki bucket S3 yang ditentukan dalam parameter. `--location` Jika GuardDuty menemukan bahwa bucket S3 ini bukan milik ID akun yang ditentukan, Anda akan mendapatkan kesalahan pada saat mengaktifkan daftar ini.

Hanya berlaku untuk ancaman kustom dan kumpulan entitas tepercaya kustom — Jika Anda memberikan URL lokasi yang tidak cocok dengan format yang didukung berikut, maka Anda akan menerima pesan galat selama penambahan daftar dan aktivasi.

Untuk memperbarui dan mengaktifkan daftar entitas ancaman

1. Jalankan UpdateThreatEntitySet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda buat daftar entitas ancaman ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

   Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).

2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut yang `name` memperbarui daftar dan juga mengaktifkan daftar ini:

   ```
   aws guardduty update-threat-entity-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganization ListEXAMPLE" \
   --threat-entity-set-id d4b94fc952d6912b8f3060768example \
   ```

```
--activate
```

Ganti `detector-id` dengan ID detektor akun anggota tempat Anda akan membuat daftar entitas ancaman, dan nilai placeholder lainnya. *shown in red*

Jika Anda tidak ingin mengaktifkan daftar yang baru dibuat ini, ganti parameternya `--activate` dengan`--no-activate`.

Parameter `expected-bucket-owner` bersifat opsional. Apakah Anda menentukan nilai untuk parameter ini atau tidak, GuardDuty memvalidasi bahwa Akun AWS ID yang terkait dengan `--detector-id` nilai ini memiliki bucket S3 yang ditentukan dalam parameter. `--location` Jika GuardDuty menemukan bahwa bucket S3 ini bukan milik ID akun yang ditentukan, Anda akan mendapatkan kesalahan pada saat mengaktifkan daftar ini.

Hanya berlaku untuk ancaman kustom dan kumpulan entitas tepercaya kustom — Jika Anda memberikan URL lokasi yang tidak cocok dengan format yang didukung berikut, maka Anda akan menerima pesan galat selama penambahan daftar dan aktivasi.

Untuk memperbarui dan mengaktifkan daftar alamat IP tepercaya

1. Jalankan CreateIPSet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda perbarui daftar alamat IP tepercaya ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

   Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).

   Untuk daftar alamat IP, nama daftar Anda harus unik di dalam Akun AWS dan Wilayah.

2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut yang juga mengaktifkan daftar:

```
aws guardduty update-ip-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--ip-set-id d4b94fc952d6912b8f3060768example \
--activate
```

Ganti `detector-id` dengan ID detektor akun anggota yang akan Anda perbarui daftar IP tepercaya, dan nilai placeholder lainnya. *shown in red*

Jika Anda tidak ingin mengaktifkan daftar yang baru dibuat ini, ganti parameternya `--activate` dengan`--no-activate`.

Parameter `expected-bucket-owner` bersifat opsional. Jika Anda tidak menentukan ID akun yang memiliki bucket S3, GuardDuty tidak akan melakukan validasi apa pun. Saat Anda menentukan ID akun untuk `expected-bucket-owner` parameter, GuardDuty validasi bahwa Akun AWS ID ini memiliki bucket S3 yang ditentukan dalam parameter. `--location` Jika GuardDuty menemukan bahwa bucket S3 ini bukan milik ID akun yang ditentukan, Anda akan mendapatkan kesalahan pada saat mengaktifkan daftar ini.

Untuk menambah dan mengaktifkan daftar IP ancaman

1. Jalankan CreateThreatIntelSet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda buat daftar alamat IP ancaman ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`

   Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).

   Untuk daftar alamat IP, nama daftar Anda harus unik di dalam Akun AWS dan Wilayah.

2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut yang juga mengaktifkan daftar:

   ```
   aws guardduty update-threat-intel-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganization ListEXAMPLE" \
   --threat-intel-set-id d4b94fc952d6912b8f3060768example \
   --activate
   ```

   Ganti `detector-id` dengan ID detektor akun anggota yang akan Anda perbarui daftar IP ancaman, dan nilai placeholder lainnya. *shown in red*

   Jika Anda tidak ingin mengaktifkan daftar yang baru dibuat ini, ganti parameternya `--activate` dengan`--no-activate`.

Parameter `expected-bucket-owner` bersifat opsional. Jika Anda tidak menentukan ID akun yang memiliki bucket S3, GuardDuty tidak akan melakukan validasi apa pun. Saat Anda menentukan ID akun untuk `expected-bucket-owner` parameter, GuardDuty validasi bahwa Akun AWS ID ini memiliki bucket S3 yang ditentukan dalam parameter. `--location` Jika GuardDuty menemukan bahwa bucket S3 ini bukan milik ID akun yang ditentukan, Anda akan mendapatkan kesalahan pada saat mengaktifkan daftar ini.

De-activating daftar entitas atau daftar alamat IP

Ketika Anda tidak lagi GuardDuty ingin menggunakan daftar, Anda dapat menonaktifkannya. Mungkin perlu beberapa menit untuk menyelesaikan proses. Untuk informasi selengkapnya, lihat Pertimbangan penting untuk daftar GuardDuty. Setelah daftar dinonaktifkan, entri dalam daftar entitas atau daftar alamat IP tidak akan memengaruhi deteksi ancaman. GuardDuty

Pilih salah satu metode akses untuk menonaktifkan daftar.

Console

Untuk menonaktifkan daftar entitas atau daftar alamat IP

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Daftar, pilih tab di mana Anda ingin menonaktifkan daftar - Daftar entitas atau daftar alamat IP.
4. Di tab yang dipilih, pilih daftar yang ingin Anda nonaktifkan.
5. Pilih Tindakan, lalu pilih Nonaktifkan.
6. Konfirmasikan tindakan dan pilih Nonaktifkan.

API/CLI

Untuk memulai dengan prosedur berikut, Anda memerlukan ID, seperti,`trustedEntitySetId`,`threatEntitySetId`, atau `trustedIpSetthreatIpSet`, yang terkait dengan sumber daya daftar yang ingin Anda nonaktifkan.

Untuk menonaktifkan daftar entitas tepercaya

1. Jalankan UpdateTrustedEntitySet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda nonaktifkan daftar entitas tepercaya ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`
2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut:

```
aws guardduty update-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

Ganti `detector-id` dengan ID detektor akun anggota tempat Anda akan menonaktifkan daftar entitas tepercaya, dan nilai placeholder lainnya. *shown in red*

Untuk menonaktifkan daftar entitas ancaman

1. Jalankan UpdateThreatEntitySet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda nonaktifkan daftar entitas ancaman ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`
2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut:

```
aws guardduty update-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--threat-entity-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

Ganti `detector-id` dengan ID detektor akun anggota tempat Anda akan membuat daftar entitas ancaman, dan nilai placeholder lainnya. *shown in red*

Untuk menonaktifkan daftar alamat IP tepercaya

1. Jalankan UpdateIPSet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda nonaktifkan daftar alamat IP tepercaya ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`
2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut dan pastikan untuk mengganti `detector-id` dengan ID detektor dari akun anggota yang Anda akan menonaktifkan daftar alamat IP tepercaya.

```
aws guardduty update-ip-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--ip-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

Untuk menonaktifkan daftar IP ancaman

1. Jalankan UpdateThreatIntelSet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda nonaktifkan daftar alamat IP ancaman ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`
2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut dan pastikan untuk mengganti `detector-id` dengan ID detektor dari akun anggota yang akan Anda nonaktifkan daftar IP ancaman.

```
aws guardduty update-threat-intel-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--threat-intel-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

Menghapus daftar entitas atau daftar alamat IP

Bila Anda tidak lagi ingin menyimpan entri daftar di set entitas atau set alamat IP Anda, Anda dapat menghapusnya. Mungkin perlu beberapa menit untuk menyelesaikan proses. Untuk informasi selengkapnya, lihat Pertimbangan penting untuk daftar GuardDuty.

Jika status daftar Mengaktifkan atau Menonaktifkan, Anda harus menunggu beberapa menit sebelum melakukan tindakan apa pun. Untuk informasi selengkapnya, lihat Memahami status daftar.

Pilih salah satu metode akses untuk menghapus daftar.

Console

Untuk menghapus daftar entitas atau daftar alamat IP

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Daftar, pilih tab di mana Anda ingin menghapus daftar - Daftar entitas atau daftar alamat IP.
4. Di tab yang dipilih, pilih daftar yang ingin Anda hapus.
5. Pilih Tindakan, lalu pilih Hapus.

   Status daftar akan berubah menjadi Hapus Tertunda. Mungkin perlu beberapa menit untuk daftar dihapus.

API/CLI

Untuk memulai dengan prosedur berikut, Anda memerlukan ID, seperti`trustedEntitySetId`,, `threatEntitySetId``trustedIpSet`, atau`threatIpSet`, yang terkait dengan sumber daya daftar yang ingin Anda hapus.

Untuk menghapus daftar entitas tepercaya

1. Jalankan DeleteTrustedEntitySet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda hapus daftar entitas tepercaya ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`
2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut:

```
aws guardduty delete-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--trusted-entity-set-id d4b94fc952d6912b8f3060768example
```

Ganti `detector-id` dengan ID detektor akun anggota tempat Anda akan menghapus daftar entitas tepercaya, dan nilai placeholder lainnya. *shown in red*

Untuk menonaktifkan daftar entitas ancaman

1. Jalankan DeleteThreatEntitySet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda hapus daftar entitas ancaman ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`
2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut:

```
aws guardduty delete-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--threat-entity-set-id d4b94fc952d6912b8f3060768example
```

Ganti `detector-id` dengan ID detektor akun anggota tempat Anda akan menghapus daftar entitas ancaman, dan nilai placeholder lainnya. *shown in red*

Untuk menghapus daftar alamat IP tepercaya

1. Jalankan DeleteIPSet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda hapus daftar alamat IP tepercaya ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`
2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut dan pastikan untuk mengganti `detector-id` dengan ID detektor dari akun anggota yang akan Anda hapus daftar alamat IP tepercaya.

```
aws guardduty delete-ip-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--ip-set-id d4b94fc952d6912b8f3060768example
```

Ganti `detector-id` dengan ID detektor akun anggota tempat Anda akan menghapus daftar entitas ancaman, dan nilai placeholder lainnya. *shown in red*

Untuk menghapus daftar IP ancaman

1. Jalankan DeleteThreatIntelSet. Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda hapus daftar alamat IP ancaman ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. `detectorId`
2. Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut dan pastikan untuk mengganti `detector-id` dengan ID detektor dari akun anggota yang akan Anda hapus daftar IP ancaman.

   ```
   aws guardduty delete-threat-intel-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --threat-intel-set-id d4b94fc952d6912b8f3060768example
   ```

   Ganti `detector-id` dengan ID detektor akun anggota tempat Anda akan menghapus daftar entitas ancaman, dan nilai placeholder lainnya. *`shown in red`*

Mengekspor GuardDuty temuan yang dihasilkan ke bucket Amazon S3

GuardDuty mempertahankan temuan yang dihasilkan untuk jangka waktu 90 hari. GuardDuty mengekspor temuan aktif ke Amazon EventBridge (EventBridge). Secara opsional, Anda dapat mengekspor temuan yang dihasilkan ke bucket Amazon Simple Storage Service (Amazon S3). Ini akan membantu Anda melacak data historis aktivitas yang berpotensi mencurigakan di akun Anda dan mengevaluasi apakah langkah perbaikan yang disarankan berhasil.

Setiap temuan aktif baru yang GuardDuty dihasilkan secara otomatis diekspor dalam waktu sekitar 5 menit setelah temuan dihasilkan. Anda dapat mengatur frekuensi untuk seberapa sering pembaruan pada temuan aktif diekspor EventBridge. Frekuensi yang Anda pilih berlaku untuk mengekspor kejadian baru dari temuan yang ada ke EventBridge, bucket S3 Anda (saat dikonfigurasi), dan Detective (saat terintegrasi). Untuk informasi tentang bagaimana menggabungkan GuardDuty beberapa kejadian dari temuan yang ada, lihat. GuardDuty menemukan agregasi

Saat Anda mengonfigurasi pengaturan untuk mengekspor temuan ke bucket Amazon S3 GuardDuty , AWS Key Management Service gunakan (AWS KMS) untuk mengenkripsi data temuan di bucket S3 Anda. Ini mengharuskan Anda menambahkan izin ke bucket S3 Anda dan AWS KMS kunci sehingga GuardDuty dapat menggunakannya untuk mengekspor temuan di akun Anda.

Daftar Isi

- Pertimbangan-pertimbangan
- Langkah 1 - Izin diperlukan untuk mengekspor temuan
- Langkah 2 - Melampirkan kebijakan ke kunci KMS Anda
- Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3
- Langkah 4 - Mengekspor temuan ke bucket S3 (Konsol)
- Langkah 5 - Mengatur frekuensi untuk mengekspor temuan aktif yang diperbarui

Pertimbangan-pertimbangan

Sebelum melanjutkan dengan prasyarat dan langkah-langkah untuk mengekspor temuan, pertimbangkan konsep-konsep kunci berikut:

- Pengaturan ekspor bersifat regional — Anda perlu mengonfigurasi opsi ekspor di setiap Wilayah tempat Anda menggunakan GuardDuty.
- Mengekspor temuan ke bucket Amazon S3 yang berbeda Wilayah AWS (Lintas wilayah) — GuardDuty mendukung pengaturan ekspor berikut:
  - Bucket atau objek Amazon S3 Anda, dan AWS KMS kunci harus milik yang sama Wilayah AWS.
  - Untuk temuan yang dihasilkan di Wilayah komersial, Anda dapat memilih untuk mengekspor temuan ini ke bucket S3 di Wilayah komersial mana pun. Namun, Anda tidak dapat mengekspor temuan ini ke bucket S3 di Wilayah opt-in.
  - Untuk temuan yang dihasilkan di Wilayah opt-in, Anda dapat memilih untuk mengekspor temuan ini ke Wilayah opt-in yang sama di mana mereka dihasilkan atau Wilayah komersial mana pun. Namun, Anda tidak dapat mengekspor temuan dari satu Wilayah pilihan ke Wilayah pilihan lain.
- Izin untuk mengekspor temuan — Untuk mengonfigurasi pengaturan untuk mengekspor temuan aktif, bucket S3 Anda harus memiliki izin yang memungkinkan GuardDuty untuk mengunggah objek. Anda juga harus memiliki AWS KMS kunci yang GuardDuty dapat digunakan untuk mengenkripsi temuan.
- Temuan yang diarsipkan tidak diekspor — Perilaku defaultnya adalah bahwa temuan yang diarsipkan, termasuk contoh baru dari temuan yang ditekan, tidak diekspor.

  Saat tem GuardDuty uan dibuat sebagai Diarsipkan, Anda harus mem batalkan arsip nya. Ini mengubah status pencarian Filter menjadi Aktif. GuardDuty mengekspor pembaruan ke temuan yang tidak diarsipkan yang ada berdasarkan cara Anda mengonfigurasiLangkah 5 — Frekuensi untuk mengekspor temuan.

- GuardDuty akun administrator dapat mengekspor temuan yang dihasilkan di akun anggota terkait — Saat Anda mengonfigurasi temuan ekspor di akun administrator, semua temuan dari akun anggota terkait yang dibuat di Wilayah yang sama juga diekspor ke lokasi yang sama yang Anda konfigurasi untuk akun administrator. Untuk informasi selengkapnya, lihat Memahami hubungan antara akun GuardDuty administrator dan akun anggota.

Langkah 1 - Izin diperlukan untuk mengekspor temuan

Saat mengonfigurasi pengaturan untuk mengekspor temuan, Anda memilih bucket Amazon S3 tempat Anda dapat menyimpan temuan dan AWS KMS kunci untuk digunakan untuk enkripsi data. Selain izin untuk GuardDuty tindakan, Anda juga harus memiliki izin untuk tindakan berikut agar berhasil mengkonfigurasi pengaturan untuk mengekspor temuan:

- `s3:GetBucketLocation`
- `s3:PutObject`

Jika Anda perlu mengekspor temuan ke awalan tertentu di bucket Amazon S3 Anda, Anda juga harus menambahkan izin berikut ke peran IAM:

- `s3:GetObject`
- `s3:ListBucket`

Langkah 2 - Melampirkan kebijakan ke kunci KMS Anda

GuardDuty mengenkripsi data temuan di bucket Anda dengan menggunakan AWS Key Management Service. Agar berhasil mengkonfigurasi pengaturan, Anda harus terlebih dahulu memberikan GuardDuty izin untuk menggunakan kunci KMS. Anda dapat memberikan izin dengan melampirkan kebijakan ke kunci KMS Anda.

Saat Anda menggunakan kunci KMS dari akun lain, Anda perlu menerapkan kebijakan kunci dengan masuk ke Akun AWS yang memiliki kunci tersebut. Saat Anda mengonfigurasi pengaturan untuk mengekspor temuan, Anda juga memerlukan kunci ARN dari akun yang memiliki kunci.

Untuk mengubah kebijakan kunci KMS GuardDuty untuk mengenkripsi temuan yang diekspor

1. Buka AWS KMS konsol di https://console.aws.amazon.com/kms.
2. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.

3. Pilih kunci KMS yang ada atau lakukan langkah-langkah untuk Membuat kunci baru di Panduan AWS Key Management Service Pengembang, yang akan Anda gunakan untuk mengenkripsi temuan yang diekspor.

> **Note**
>
> K Wilayah AWS unci KMS Anda dan bucket Amazon S3 harus sama.

Anda dapat menggunakan bucket S3 dan pasangan kunci KMS yang sama untuk mengekspor temuan dari Wilayah yang berlaku. Untuk informasi selengkapnya, lihat Pertimbangan-pertimbangan untuk mengekspor temuan di seluruh Wilayah.

4. Di bagian Kebijakan utama, pilih Edit.

Jika Tampilan Beralih ke kebijakan ditampilkan, pilih untuk menampilkan kebijakan Kunci, lalu pilih Edit.

5. Salin blok kebijakan berikut ke kebijakan kunci KMS Anda, untuk memberikan GuardDuty izin untuk menggunakan kunci Anda.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

6. Edit kebijakan dengan mengganti nilai-nilai berikut yang diformat *red* dalam contoh kebijakan:

1. Ganti *KMS key ARN* dengan Nama Sumber Daya Amazon (ARN) dari kunci KMS. Untuk menemukan kunci ARN, lihat M enemukan ID kunci dan ARN di Panduan AWS Key Management Service Pengembang.
2. Ganti *123456789012* dengan Akun AWS ID yang memiliki GuardDuty akun yang mengekspor temuan.
3. Ganti *Region2* dengan Wilayah AWS tempat tem GuardDuty uan dihasilkan.
4. Ganti *SourceDetectorID* dengan `detectorID` GuardDuty akun di Wilayah tertentu tempat temuan dihasilkan.

   Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`

> **Note**
>
> Jika Anda menggunakan GuardDuty di Wilayah opt-in, ganti nilai untuk “Layanan” dengan titik akhir Regional untuk Wilayah tersebut. Misalnya, jika Anda menggunakan GuardDuty di Wilayah Timur Tengah (Bahrain) (me-south-1), ganti `"Service": "guardduty.amazonaws.com"` dengan. `"Service": "guardduty.me-south-1.amazonaws.com"` Untuk informasi tentang titik akhir untuk setiap Wilayah pilihan, lihat titik akhir dan kuota GuardDuty .

7. Jika Anda menambahkan pernyataan kebijakan sebelum pernyataan akhir, tambahkan koma sebelum menambahkan pernyataan ini. Pastikan sintaks JSON kebijakan kunci KMS Anda valid.

   Pilih Simpan.
8. (Opsional) salin kunci ARN ke notepad untuk digunakan pada langkah selanjutnya.

Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3

Tambahkan izin ke bucket Amazon S3 tempat Anda akan mengekspor temuan sehingga GuardDuty dapat mengunggah objek ke bucket S3 ini. Terlepas dari penggunaan bucket Amazon S3 yang dimiliki akun Anda atau di akun lain Akun AWS, Anda harus menambahkan izin ini.

Jika suatu saat, Anda memutuskan untuk mengekspor temuan ke bucket S3 yang berbeda, maka untuk melanjutkan mengekspor temuan, Anda harus menambahkan izin ke bucket S3 tersebut dan mengonfigurasi setelan temuan ekspor lagi.

Jika Anda belum memiliki bucket Amazon S3 tempat Anda ingin mengekspor temuan ini, lihat Membuat bucket di Panduan Pengguna Amazon S3.

Untuk melampirkan izin ke kebijakan bucket S3 Anda

1. Lakukan langkah-langkah di bawah Membuat atau mengedit kebijakan bucket di Panduan Pengguna Amazon S3, hingga halaman Edit kebijakan bucket muncul.
2. Kebijakan contoh menunjukkan cara memberikan GuardDuty izin untuk mengekspor temuan ke bucket Amazon S3 Anda. Jika Anda mengubah jalur setelah mengonfigurasi temuan ekspor, Anda harus mengubah kebijakan untuk memberikan izin ke lokasi baru.

   Salin contoh kebijakan berikut dan tempelkan ke editor kebijakan Bucket.

   Jika Anda menambahkan pernyataan kebijakan sebelum pernyataan akhir, tambahkan koma sebelum menambahkan pernyataan ini. Pastikan sintaks JSON kebijakan kunci KMS Anda valid.

   Kebijakan contoh bucket S3

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Allow GetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
```

```
            "Sid": "Allow PutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "Deny unencrypted object uploads",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "Deny incorrect encryption header",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
                "StringNotEquals": {
```

```
                "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:us-east-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

3. Edit kebijakan dengan mengganti nilai-nilai berikut yang diformat *red* dalam contoh kebijakan:

   1. Ganti *Amazon S3 bucket ARN* dengan Nama Sumber Daya Amazon (ARN) dari bucket Amazon S3. Anda dapat menemukan Bucket ARN di halaman kebijakan Edit bucket di https://console.aws.amazon.com/s3/ konsol.
   2. Ganti *123456789012* dengan Akun AWS ID yang memiliki GuardDuty akun yang mengekspor temuan.
   3. Ganti *us-east-2* dengan Wilayah AWS tempat tem GuardDuty uan dihasilkan.
   4. Ganti *SourceDetectorID* dengan `detectorID` GuardDuty akun di Wilayah tertentu tempat temuan dihasilkan.

      Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Peng aturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. `detectorId`
   5. Ganti *[optional prefix]* bagian dari nilai *S3 bucket ARN/[optional prefix]* placeholder dengan lokasi folder opsional tempat Anda ingin mengekspor temuan. Untuk informasi selengkapnya tentang penggunaan awalan, lihat Meng atur objek menggunakan awalan di Panduan Pengguna Amazon S3.

Bila Anda memberikan lokasi folder opsional, folder tersebut harus sudah ada di bucket S3. GuardDuty tidak membuat folder atas nama Anda. Persyaratan ini berlaku terlepas dari kepemilikan bucket.

6. Ganti *KMS key ARN* dengan Amazon Resource Name (ARN) dari kunci KMS yang terkait dengan enkripsi temuan yang diekspor ke bucket S3. Untuk menemukan kunci ARN, lihat M enemukan ID kunci dan ARN di Panduan AWS Key Management Service Pengembang.

> **Note**
>
> Jika Anda menggunakan GuardDuty di Wilayah opt-in, ganti nilai untuk “Layanan” dengan titik akhir Regional untuk Wilayah tersebut. Misalnya, jika Anda menggunakan GuardDuty di Wilayah Timur Tengah (Bahrain) (me-south-1), ganti `"Service": "guardduty.amazonaws.com"` dengan. `"Service": "guardduty.me-south-1.amazonaws.com"` Untuk informasi tentang titik akhir untuk setiap Wilayah pilihan, lihat titik akhir dan kuota GuardDuty .

4. Pilih Simpan.

Langkah 4 - Mengekspor temuan ke bucket S3 (Konsol)

GuardDuty memungkinkan Anda untuk mengekspor temuan ke bucket yang ada di bucket lain Akun AWS.

Saat membuat bucket S3 baru atau memilih bucket yang ada di akun Anda, Anda dapat menambahkan awalan opsional. Baik awalan dan jalur folder tempat temuan ditulis harus sudah ada di bucket S3. GuardDuty tidak membuat folder apa pun atas nama Anda. GuardDuty menulis objek temuan ke jalur`/AWSLogs/`*`123456789012`*`/GuardDuty/`*`Region`*, jadi Anda harus membuat struktur folder ini sebelum Anda mengekspor temuan.

Seluruh jalur objek S3 akan menjadi*`amzn-s3-demo-bucket`*`/`*`prefix-name`*`/UUID`*`.jsonl.gz`*. Di `UUID` buat secara acak dan tidak mewakili ID detektor atau ID temuan.

> **Important**
>
> Kunci KMS dan bucket S3 harus berada di Wilayah yang sama.

Sebelum menyelesaikan langkah-langkah ini, pastikan Anda telah melampirkan kebijakan masing-masing ke kunci KMS dan bucket S3 yang ada.

Untuk mengonfigurasi temuan ekspor

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pada halaman Peng aturan, di bawah Opsi ekspor Find ings, untuk bucket S3, pilih Konfigurasikan sekarang (atau Edit, sesuai kebutuhan).
4. Untuk bucket S3 ARN, masukkan**`bucket ARN`**. Untuk menemukan bucket ARN, lihat Melihat properti untuk bucket S3 di Panduan Pengguna Amazon S3.
5. Untuk kunci KMS ARN, masukkan. **`key ARN`** Untuk menemukan kunci ARN, lihat M enemukan ID kunci dan ARN di Panduan AWS Key Management Service Pengembang.
6. Lampirkan kebijakan
   - Lakukan langkah-langkah untuk melampirkan kebijakan bucket S3. Untuk informasi selengkapnya, lihat Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3.
   - Lakukan langkah-langkah untuk melampirkan kebijakan kunci KMS. Untuk informasi selengkapnya, lihat Langkah 2 - Melampirkan kebijakan ke kunci KMS Anda.
7. Pilih Simpan.

Langkah 5 - Mengatur frekuensi untuk mengekspor temuan aktif yang diperbarui

Konfigurasikan frekuensi untuk mengekspor temuan aktif yang diperbarui sesuai dengan lingkungan Anda. Secara default, temuan yang diperbarui diekspor setiap 6 jam. Ini berarti bahwa setiap temuan yang diperbarui setelah ekspor terbaru akan disertakan dalam ekspor berikutnya. Jika temuan yang diperbarui diekspor setiap 6 jam dan ekspor dilakukan pada pukul 12:00, setiap temuan yang Anda perbarui setelah pukul 12:00 akan diekspor pada pukul 18:00.

Untuk mengatur frekuensi

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Pilih Pengaturan.

3. Di bagian Opsi ekspor Temuan, pilih Fre kuensi untuk temuan yang diperbarui. Ini menetapkan frekuensi untuk mengekspor temuan Aktif yang diperbarui ke keduanya EventBridge dan Amazon S3. Anda dapat memilih dari opsi berikut:

   - Perbarui EventBridge dan S3 setiap 15 menit
   - Update EventBridge dan S3 setiap 1 jam
   - Perbarui EventBridge dan S3 setiap 6 jam (default)

4. Pilih Simpan perubahan.

Memproses GuardDuty temuan dengan Amazon EventBridge

GuardDuty secara otomatis menerbitkan (mengirim) temuan sebagai peristiwa ke Amazon EventBridge (sebelumnya CloudWatch Amazon Events), layanan bus acara tanpa server. EventBridge mengirimkan aliran data hampir real-time dari aplikasi dan layanan ke target seperti topik, fungsi, dan aliran Amazon Simple Notification Service (Amazon SNS), fungsi, AWS Lambda dan Amazon Kinesis. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

EventBridge memungkinkan pemantauan dan pemrosesan GuardDuty temuan secara otomatis dengan menerima acara. EventBridge menerima peristiwa untuk temuan yang baru dihasilkan dan temuan agregat, di mana kejadian selanjutnya dari temuan yang ada digabungkan dengan aslinya. Setiap GuardDuty temuan diberi ID temuan, dan GuardDuty membuat EventBridge acara untuk setiap temuan dengan ID temuan unik. Untuk informasi tentang cara kerja agregasi GuardDuty, lihatGuardDuty menemukan agregasi.

Selain pemantauan dan pemrosesan otomatis, penggunaan EventBridge memungkinkan retensi jangka panjang dari data temuan Anda. GuardDuty menyimpan temuan selama 90 hari. Dengan EventBridge, Anda dapat mengirim data temuan ke platform penyimpanan pilihan Anda dan menyimpan data selama yang Anda suka. Untuk mempertahankan temuan untuk durasi yang lebih lama, GuardDuty mendukungMengekspor temuan yang dihasilkan ke Amazon S3.

Topik

- Memahami frekuensi EventBridge notifikasi di GuardDuty
- Siapkan topik dan titik akhir Amazon SNS (Email, Slack, dan Amazon Chime)
- Menggunakan Amazon EventBridge untuk GuardDuty temuan
- Membuat EventBridge aturan untuk GuardDuty temuan
- EventBridge aturan untuk lingkungan GuardDuty multi-akun

Memahami frekuensi EventBridge notifikasi di GuardDuty

Bagian ini menjelaskan seberapa sering Anda menerima pemberitahuan pencarian melalui EventBridge dan cara memperbarui frekuensi untuk kejadian temuan berikutnya.

Pemberitahuan untuk temuan yang baru dibuat dengan ID temuan unik

GuardDuty mengirimkan notifikasi ini dalam waktu dekat saat menghasilkan temuan dengan ID temuan unik. Pemberitahuan mencakup semua kejadian berikutnya dari ID temuan ini selama proses pembuatan notifikasi.

Frekuensi notifikasi untuk temuan yang baru dihasilkan mendekati waktu nyata. Secara default, Anda tidak dapat memodifikasi frekuensi ini.

Pemberitahuan untuk kejadian temuan selanjutnya

GuardDuty menggabungkan semua kejadian berikutnya dari jenis temuan tertentu yang terjadi dalam interval 6 jam menjadi satu peristiwa tunggal. Hanya akun administrator yang dapat memperbarui frekuensi EventBridge notifikasi untuk kejadian penemuan berikutnya. Akun anggota tidak dapat memperbarui frekuensi ini untuk akun mereka sendiri. Misalnya, jika akun GuardDuty administrator yang didelegasikan memperbarui frekuensi menjadi satu jam, semua akun anggota juga akan memiliki frekuensi pemberitahuan satu jam tentang kejadian temuan berikutnya yang dikirim ke. EventBridge Untuk informasi selengkapnya, lihat Mengelola banyak akun di Amazon GuardDuty.

Sebagai akun administrator, Anda dapat menyesuaikan frekuensi default pemberitahuan tentang kejadian temuan berikutnya. Nilai yang mungkin adalah 15 menit, 1 jam, atau default 6 jam. Untuk informasi tentang menyetel frekuensi notifikasi ini, lihatLangkah 5 - Mengatur frekuensi untuk mengekspor temuan aktif yang diperbarui.

Untuk detail selengkapnya tentang akun administrator yang menerima EventBridge pemberitahuan untuk akun anggota, lihatEventBridge aturan untuk lingkungan multi-akun.

Siapkan topik dan titik akhir Amazon SNS (Email, Slack, dan Amazon Chime)

Amazon Simple Notification Service (Amazon SNS) adalah layanan terkelola penuh yang menyediakan pengiriman pesan dari penerbit ke pelanggan. Penerbit berkomunikasi secara asinkron dengan pelanggan dengan mengirim pesan ke suatu topik. Topik adalah jalur akses logis dan saluran

komunikasi yang memungkinkan Anda mengelompokkan beberapa titik akhir seperti AWS Lambda, Amazon Simple Queue Service (Amazon HTTP/S SQS), dan alamat email.

> **Note**
>
> Anda dapat menambahkan topik Amazon SNS ke aturan EventBridge acara pilihan Anda selama atau setelah pembuatan aturan.

Buat topik Amazon SNS

Untuk memulai, Anda harus terlebih dahulu menyiapkan topik di Amazon SNS dan menambahkan titik akhir. Untuk membuat topik, lakukan langkah-langkah di Langkah 1: Membuat topik di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Setelah topik dibuat, salin topik ARN ke clipboard. Anda akan menggunakan topik ini ARN untuk melanjutkan dengan salah satu pengaturan yang disukai.

Pilih metode yang disukai untuk menentukan di mana Anda ingin mengirim data GuardDuty pencarian.

Email setup

Untuk menyiapkan titik akhir email

Setelah AndaCreate an Amazon SNS topic, langkah selanjutnya adalah membuat langganan topik ini. Lakukan langkah-langkah di bawah Langkah 2: Membuat langganan ke topik Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

1. Untuk Topik ARN, gunakan topik ARN yang dibuat di langkah. Create an Amazon SNS topic Topik ARN terlihat mirip dengan yang berikut:

   ```
   arn:aws:sns:us-east-2:123456789012:your_topic
   ```

2. Untuk Protokol, pilih Email.
3. Untuk Endpoint, masukkan alamat email tempat Anda ingin menerima notifikasi dari Amazon SNS.

   Setelah langganan dibuat, Anda harus mengonfirmasinya melalui klien email Anda.

Slack setup

Untuk mengkonfigurasi Pengembang Amazon Q di klien aplikasi obrolan - Slack

Setelah AndaCreate an Amazon SNS topic, langkah selanjutnya adalah mengkonfigurasi klien untuk Slack.

Lakukan langkah-langkah di bawah Tutorial: Mulai dengan Slack di Pengembang Amazon Q di aplikasi obrolan Panduan Administrator.

Chime setup

Untuk mengkonfigurasi Pengembang Amazon Q di klien aplikasi obrolan - Chime

Setelah AndaCreate an Amazon SNS topic, langkah selanjutnya adalah mengonfigurasi Pengembang Amazon Q untuk Chime.

Lakukan langkah-langkah di bawah Tutorial: Mulai dengan Amazon Chime di Pengembang Amazon Q dalam aplikasi obrolan Panduan Administrator.

Menggunakan Amazon EventBridge untuk GuardDuty temuan

Dengan EventBridge, Anda membuat aturan untuk menentukan peristiwa yang ingin Anda pantau. Aturan ini juga menentukan layanan target dan aplikasi yang dapat melakukan tindakan otomatis jika peristiwa ini terjadi. Target adalah tujuan (sumber daya atau titik akhir) yang EventBridge mengirimkan peristiwa ke saat acara cocok dengan pola acara yang ditentukan dalam aturan. Setiap peristiwa adalah objek JSON yang sesuai dengan EventBridge skema untuk AWS peristiwa dan berisi representasi JSON dari sebuah temuan. Anda dapat menyesuaikan aturan untuk mengirim hanya acara-acara yang memenuhi kriteria tertentu. Untuk informasi selengkapnya, lihat the section called “Skema peristiwa”. Karena data temuan disusun sebagai suatu EventBridgeperistiwa, Anda dapat memantau, memproses, dan menindaklanjuti temuan dengan menggunakan aplikasi, layanan, dan alat lain.

Untuk menerima pemberitahuan tentang GuardDuty temuan berdasarkan peristiwa, Anda harus membuat EventBridge aturan dan target untuk GuardDuty. Aturan ini memungkinkan EventBridge untuk mengirim pemberitahuan untuk temuan yang GuardDuty menghasilkan target yang ditentukan dalam aturan.

> **Note**
>
> EventBridge dan CloudWatch Acara adalah layanan dan API dasar yang sama. Namun, EventBridge termasuk fitur tambahan yang membantu Anda menerima acara dari aplikasi perangkat lunak sebagai layanan (SaaS) dan aplikasi Anda sendiri. Karena layanan dan API yang mendasarinya sama, skema peristiwa untuk GuardDuty temuan juga sama.

Bagaimana temuan yang diarsipkan dan tidak diarsipkan bekerja dengan GuardDuty EventBridge

Untuk temuan yang Anda arsipkan secara manual, kejadian awal dan semua kejadian selanjutnya dari temuan ini (dihasilkan setelah pengarsipan selesai) dikirim EventBridge berdasarkan frekuensi pemberitahuan tertentu. Untuk informasi selengkapnya, lihat Memahami frekuensi EventBridge notifikasi di GuardDuty.

Untuk temuan yang secara otomatis diarsipkan dengan Aturan penekanan, awal dan semua kejadian selanjutnya dari temuan ini (dihasilkan setelah pengarsipan selesai) tidak dikirim ke. EventBridge Anda dapat melihat temuan yang diarsipkan secara otomatis ini di GuardDuty konsol.

Skema peristiwa

Pola peristiwa mendefinisikan data yang EventBridge digunakan untuk menentukan apakah akan mengirim acara ke target. EventBridgeAcara untuk GuardDuty memiliki format sebagai berikut:

```
{
        "version": "0",
        "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
        "detail-type": "GuardDuty Finding",
        "source": "aws.guardduty",
        "account": "111122223333",
        "time": "1970-01-01T00:00:00Z",
        "region": "us-east-1",
        "resources": [],
        "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
       }
```

`detail`Nilai mengembalikan rincian JSON dari temuan tunggal sebagai objek, sebagai lawan mengembalikan seluruh sintaks respons temuan yang mendukung beberapa temuan dalam array.

Untuk daftar lengkap semua parameter yang disertakan`GUARDDUTY_FINDING_JSON_OBJECT`, lihat GetFindings. Parameter `id` yang muncul di `GUARDDUTY_FINDING_JSON_OBJECT` adalah ID temuan yang telah dijelaskan sebelumnya.

Membuat EventBridge aturan untuk GuardDuty temuan

Prosedur berikut menjelaskan cara menggunakan EventBridge konsol Amazon dan AWS Command Line Interface (AWS CLI) untuk membuat EventBridge aturan untuk GuardDuty temuan. Aturan mendeteksi EventBridge peristiwa yang menggunakan skema dan pola peristiwa untuk GuardDuty temuan, dan mengirimkan peristiwa tersebut ke AWS Lambda fungsi untuk diproses.

AWS Lambda adalah layanan komputasi yang dapat Anda gunakan untuk menjalankan kode tanpa menyediakan atau mengelola server. Anda mengemas kode Anda dan mengunggahnya AWS Lambda sebagai fungsi Lambda. AWS Lambda kemudian menjalankan fungsi ketika fungsi dipanggil. Fungsi dapat dipanggil secara manual oleh Anda, secara otomatis dalam respons terhadap peristiwa, atau dalam merespons atas permintaan dari aplikasi atau layanan. Untuk informasi tentang membuat dan memanggil fungsi Lambda, lihat Panduan Developer AWS Lambda.

Pilih metode pilihan Anda untuk membuat EventBridge aturan yang mengirimkan GuardDuty temuan Anda ke target.

Console

Ikuti langkah-langkah berikut untuk menggunakan EventBridge konsol Amazon untuk membuat aturan yang secara otomatis mengirimkan semua peristiwa GuardDuty pencarian ke fungsi Lambda untuk diproses. Aturan menggunakan pengaturan default untuk aturan yang berjalan saat peristiwa tertentu diterima. Untuk detail tentang setelan aturan atau mempelajari cara membuat aturan yang menggunakan setelan khusus, lihat Membuat aturan yang bereaksi terhadap peristiwa di Panduan EventBridge Pengguna Amazon.

Sebelum Anda membuat aturan ini, buat fungsi Lambda yang Anda inginkan aturan tersebut digunakan sebagai target. Saat Anda membuat aturan tersebut, Anda harus menentukan fungsi ini sebagai target aturan. Target Anda juga bisa menjadi topik SNS yang Anda buat sebelumnya. Untuk informasi selengkapnya, lihat Siapkan topik dan titik akhir Amazon SNS (Email, Slack, dan Amazon Chime).

Untuk membuat aturan acara dengan menggunakan konsol

1. Masuk ke Konsol Manajemen AWS dan buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.

2. Di panel navigasi, di bawah Bus, pilih Aturan.
3. Di bagian Aturan, pilih Buat aturan.
4. Pada halaman Define rule detail, lakukan hal berikut:
    a. Untuk Nama, masukkan nama untuk aturan.
    b. (Opsional) Untuk Deskripsi, masukkan deskripsi singkat tentang aturan.
    c. Untuk bus Acara, pastikan bahwa default dipilih dan Aktifkan aturan pada bus acara yang dipilih diaktifkan.
    d. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
    e. Setelah selesai, pilih Selanjutnya.
5. Pada halaman pola acara Build, lakukan hal berikut:
    a. Untuk sumber Acara, pilih AWS acara atau acara EventBridge mitra.
    b. (Opsional) Untuk acara Sampel, tinjau peristiwa pencarian sampel GuardDuty untuk mempelajari apa yang mungkin terkandung dalam suatu peristiwa. Untuk melakukan ini, pilih AWS acara. Kemudian, untuk acara Contoh, pilih GuardDutyMenemukan.
    c. Opsi 1 - Menggunakan formulir pola, template yang EventBridge menyediakan

        Di bagian Pola acara, Anda dapat melakukan hal berikut:

        1. Untuk metode Creation, pilih Gunakan formulir pola.
        2. Untuk Sumber peristiwa, pilih Layanan AWS.
        3. Untuk Layanan AWS, pilih GuardDuty.
        4. Untuk jenis Event, pilih GuardDuty Finding.

        Setelah selesai, pilih Selanjutnya.
    d. Opsi 2 - Menggunakan pola acara kustom di JSON

        Di bagian Pola acara, Anda dapat melakukan hal berikut:

        1. Untuk metode Creation, pilih Custom pattern (JSON editor).
        2. Untuk pola Peristiwa, tempel JSON kustom berikut yang akan membuat peringatan untuk temuan sedang, tinggi, dan kritis. Untuk informasi selengkapnya, lihat Tingkat keparahan temuan.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
      5,
      5.0,
      5.1,
      5.2,
      5.3,
      5.4,
      5.5,
      5.6,
      5.7,
      5.8,
      5.9,
      6,
      6.0,
      6.1,
      6.2,
      6.3,
      6.4,
      6.5,
      6.6,
      6.7,
      6.8,
      6.9,
      7,
```

```
      7.0,
      7.1,
      7.2,
      7.3,
      7.4,
      7.5,
      7.6,
      7.7,
      7.8,
      7.9,
      8,
      8.0,
      8.1,
      8.2,
      8.3,
      8.4,
      8.5,
      8.6,
      8.7,
      8.8,
      8.9,
      9,
      9.0,
      9.1,
      9.2,
      9.3,
      9.4,
      9.5,
      9.6,
      9.7,
      9.8,
      9.9,
      10,
      10.0
    ]
  }
}
```

Setelah selesai, pilih Selanjutnya.

6. Opsi A - Memilih Layanan AWS - AWS Lambda sebagai target

   Pada halaman Pilih target, lakukan hal berikut:

a. Untuk jenis Target, pilih Layanan AWS.

b. Untuk Pilih target, pilih Fungsi Lambda. Kemudian, untuk Fungsi, pilih fungsi Lambda yang ingin Anda kirimi acara pencarian.

c. Untuk Konfigurasi version/alias, masukkan pengaturan versi atau alias untuk fungsi Lambda target.

d. (Opsional) Untuk Pengaturan tambahan, masukkan pengaturan khusus untuk menentukan data peristiwa mana yang ingin Anda kirim ke fungsi Lambda. Anda juga dapat menentukan cara menangani peristiwa yang tidak berhasil dikirim ke fungsi.

e. Setelah selesai, pilih Selanjutnya.

7. Opsi B - Memilih topik SNS sebagai target

   Pada halaman Pilih target, lakukan hal berikut:

   a. Untuk jenis Target, pilih Layanan AWS.

   b. Untuk Pilih target, pilih Topik SNS. Kemudian, untuk lokasi Target, pilih opsi yang sesuai berdasarkan lokasi target Anda. Untuk Topik, pilih nama topik SNS yang Anda buat.

   c. Perluas Pengaturan tambahan. Untuk Konfigurasi input target, pilih Trafo input.

   d. Pilih Konfigurasi transformator input.

   e. Salin kode berikut dan tempel di bidang Input Path di bawah bagian Transformator input target.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_Description": "$.detail.description"
}
```

   f. Salin kode berikut dan tempel ke bidang Template untuk memformat email.

```
{"message":"You have a severity <severity> GuardDuty finding type
 <Finding_Type> in the <region> Region.\n\nFinding Description:
\n<Finding_Description>\n\nFor more details open the GuardDuty console at
```

```
 https://console.aws.amazon.com/guardduty/home?region=<region>#/findings?
search=id%3D<Finding_ID>"}
```

> **Important**
>
> Berikan template sebagai objek JSON satu baris, dengan pesan dibungkus dalam kunci sepertimessage, seperti yang ditunjukkan pada contoh sebelumnya. Gunakan \n untuk menambahkan jeda baris.
> GuardDuty menemukan bidang seperti description dapat berisi karakter kontrol yang tidak terlolos, termasuk baris baru. Jangan gunakan salah satu format template berikut:
>
> - String yang dikutip telanjang
> - Template multi-baris yang menggunakan string kutipan terpisah pada baris terpisah
>
> Dengan format ini, nilai substitusi dapat menghasilkan JSON yang tidak valid. EventBridge kemudian menolak acara dan tidak mengirimkan pemberitahuan.

> **Note**
>
> Langganan email menerima output template apa adanya, sehingga email menunjukkan objek message JSON, dan jeda baris muncul sebagai. \n Untuk notifikasi yang diformat, kirimkan topik Amazon SNS ke Pengembang Amazon Q di aplikasi obrolan (Slack atau Amazon Chime), atau gunakan fungsi Lambda sebagai target.

8. Pada halaman Konfigurasi tag, secara opsional masukkan satu atau beberapa tag untuk ditetapkan ke aturan. Lalu pilih Selanjutnya.
9. Pada halaman Tinjau dan buat, tinjau setelan aturan dan verifikasi apakah sudah benar.

   Untuk mengubah pengaturan, pilih Edit di bagian yang berisi pengaturan, lalu masukkan pengaturan yang benar. Anda juga dapat menggunakan tab navigasi untuk membuka halaman yang berisi pengaturan.
10. Setelah selesai memverifikasi pengaturan, pilih Buat aturan.

API

Prosedur berikut menunjukkan cara menggunakan AWS CLI perintah untuk membuat EventBridge aturan dan target untuk GuardDuty. Secara khusus, prosedur ini menunjukkan kepada Anda cara membuat aturan yang memungkinkan EventBridge untuk mengirim peristiwa untuk semua temuan yang GuardDuty menghasilkan AWS Lambda fungsi sebagai target aturan.

> **Note**
>
> Dalam contoh ini, kita menggunakan fungsi Lambda sebagai target untuk aturan yang memicu. EventBridge Anda juga dapat mengonfigurasi AWS sumber daya lain sebagai target yang akan dipicu EventBridge. GuardDuty dan EventBridge mendukung jenis target berikut - instans Amazon EC2, aliran Amazon Kinesis, tugas Amazon ECS, mesin status AWS Step Functions , perintah, dan target bawaan. `run` Untuk informasi selengkapnya, lihat PutTargetsdi Referensi Amazon EventBridge API.

Untuk membuat aturan dan target

1. Untuk membuat aturan yang memungkinkan EventBridge untuk mengirim peristiwa untuk semua temuan yang GuardDuty dihasilkan, jalankan perintah EventBridge CLI berikut.

   ```
   aws events put-rule --name your-rule-name --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

   Anda dapat menyesuaikan aturan Anda lebih lanjut sehingga menginstruksikan EventBridge untuk mengirim acara hanya untuk sebagian dari temuan. GuardDuty-generated Subset ini didasarkan pada atribut temuan atau atribut yang ditentukan dalam aturan. Misalnya, gunakan perintah CLI berikut untuk membuat aturan yang memungkinkan EventBridge untuk hanya mengirim peristiwa untuk GuardDuty temuan dengan tingkat keparahan 5 atau 8:

   ```
   aws events put-rule --name your-rule-name --event-pattern "{\"source\":
   [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],\"detail\":
   {\"severity\":[5,8]}}"
   ```

   Untuk tujuan ini, Anda dapat menggunakan salah satu nilai properti yang tersedia di JSON untuk GuardDuty temuan.

2. Untuk melampirkan fungsi Lambda sebagai target untuk aturan yang Anda buat di langkah 1, jalankan perintah CLI berikut EventBridge .

```
aws events put-targets --rule your-rule-name --targets
 Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:your-function
```

Pastikan untuk mengganti `your-rule-name` dengan nama aturan yang Anda buat di langkah 1, dan `your-function` dengan fungsi Lambda Anda yang sebenarnya untuk acara tersebut GuardDuty .

3. Untuk menambahkan izin yang diperlukan untuk memanggil target, jalankan perintah CLI Lambda berikut.

```
aws lambda add-permission --function-name your-function --statement-id 1 --
action 'lambda:InvokeFunction' --principal events.amazonaws.com --source-arn
 arn:aws:events:us-east-1:111122223333:rule/your-rule-name
```

Pastikan untuk mengganti `your-function` dengan fungsi Lambda Anda yang sebenarnya untuk GuardDuty acara tersebut, dan `your-rule-name` dengan nama aturan yang Anda buat di langkah 1. `--source-arn`Kondisi ini hanya mengizinkan aturan ini untuk memanggil fungsi.

EventBridge aturan untuk lingkungan GuardDuty multi-akun

Saat menggunakan akun GuardDuty administrator yang didelegasikan, Anda dapat melihat peristiwa yang dihasilkan di akun anggota dan mengambil tindakan menggunakan aplikasi dan layanan lain. EventBridge aturan di akun administrator Anda akan dipicu berdasarkan temuan yang berlaku dari akun anggota Anda. Jika Anda mengatur pencarian notifikasi melalui EventBridge akun administrator Anda, Anda akan menerima pemberitahuan temuan dari akun dan akun anggota Anda. Misalnya, Anda dapat menggunakan EventBridge untuk mengirim jenis temuan tertentu ke fungsi Lambda yang memproses dan mengirim data ke sistem manajemen insiden dan peristiwa keamanan (SIEM) Anda.

Anda dapat mengidentifikasi akun anggota tempat GuardDuty temuan itu berasal menggunakan `accountId` bidang detail JSON temuan. Untuk membuat aturan acara khusus untuk akun anggota tertentu, buat aturan baru dan gunakan templat berikut dalam pola Acara. Ganti *123456789012* dengan akun anggota yang ingin Anda picu acara. `accountId`

```
{
```

```
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> Contoh ini membuat aturan yang cocok dengan semua temuan dari ID akun yang ditentukan. Anda dapat menyertakan beberapa ID akun dengan memisahkannya dengan koma, mengikuti sintaks JSON.

Memahami CloudWatch Log dan alasan melewatkan sumber daya selama Perlindungan Malware untuk pemindaian EC2

GuardDuty Perlindungan Malware untuk EC2 menerbitkan peristiwa ke grup CloudWatch log Amazon Anda aws/guardduty/malware-scan-events. Untuk setiap peristiwa yang terkait dengan pemindaian malware, Anda dapat memantau status dan hasil pemindaian sumber daya yang terkena dampak. Sumber daya Amazon EC2 tertentu dan volume Amazon EBS mungkin telah dilewati selama pemindaian Perlindungan Malware untuk EC2.

Mengaudit CloudWatch Log dalam Per GuardDuty lindungan Malware untuk EC2

Ada tiga jenis peristiwa pemindaian yang didukung dalam grup log aws/guardduty /malware-scan-events CloudWatch .

Perlindungan Malware untuk nama acara pemindaian EC2	Penjelasan
`EC2_SCAN_STARTED`	Dibuat saat GuardDuty Perlindungan Malware untuk EC2 memulai proses pemindaian malware, seperti bersiap untuk mengambil snapshot volume EBS.
`EC2_SCAN_COMPLETED`	Dibuat saat GuardDuty Perlindungan Malware untuk pemindaian EC2 selesai untuk setidaknya satu volume EBS dari sumber daya yang terkena dampak. Acara ini juga mencakup `snapshotId` yang termasuk dalam volume EBS yang dipindai. Setelah pemindaian selesai, hasil pemindaian akan menjadi`CLEAN`,`THREATS_FOUND` , atau`NOT_SCANNED` .
`EC2_SCAN_SKIPPED`	Dibuat saat GuardDuty Perlindungan Malware untuk pemindaian EC2 melewatkan semua volume EBS dari sumber daya yang terkena dampak. Untuk mengidentifikasi alasan lewat, pilih acara yang sesuai, dan lihat detailnya . Untuk informasi lebih lanjut tentang alasan melewatkan, lihat Alasan melewatkan sumber daya selama pemindaian malware di bawah.

> **Note**
>
> Jika Anda menggunakan AWS Organizations, CloudWatch log peristiwa dari akun anggota di Organisasi akan dipublikasikan ke akun administrator dan grup log akun anggota.

Pilih metode akses pilihan Anda untuk melihat dan menanyakan CloudWatch peristiwa.

Console

1. Masuk ke Konsol Manajemen AWS dan buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, di bawah Log, pilih Grup log. Pilih grup log aws/guardduty /malware-scan-events untuk melihat peristiwa pemindaian untuk Perlindungan GuardDuty Malware untuk EC2.

   Untuk menjalankan kueri, pilih Log Insights.

   Untuk informasi tentang menjalankan kueri, lihat Meng analisis data CloudWatch log dengan Logs Insights di Panduan CloudWatch Pengguna Amazon.
3. Pilih Scan ID untuk memantau detail sumber daya yang terkena dampak dan temuan malware. Misalnya, Anda dapat menjalankan kueri berikut untuk memfilter peristiwa CloudWatch log dengan menggunakan`scanId`. Pastikan untuk menggunakan valid Anda sendiri*scan-id*.

   ```
   fields @timestamp, @message, scanRequestDetails.scanId as scanId
   | filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
   | sort @timestamp asc
   ```

API/CLI

- Untuk bekerja dengan grup log, lihat Pencarian entri log menggunakan AWS CLI di Panduan CloudWatch Pengguna Amazon.

  Pilih grup log aws/guardduty /malware-scan-events untuk melihat peristiwa pemindaian untuk Perlindungan GuardDuty Malware untuk EC2.
- Untuk melihat dan memfilter peristiwa log, lihat GetLogEvents dan FilterLogEvents, masing-masing, di Refer ensi CloudWatch API Amazon.

GuardDuty Perlindungan Malware untuk retensi log EC2

Periode penyimpanan log default untuk grup log aws/guardduty /malware-scan-events adalah 90 hari, setelah itu peristiwa log dihapus secara otomatis. Untuk mengubah kebijakan penyimpanan log untuk grup CloudWatch log Anda, lihat Meng ubah retensi data CloudWatch log di Log di Panduan CloudWatch Pengguna Amazon, atau PutRetentionPolicy di Refer ensi CloudWatch API Amazon.

Alasan melewatkan sumber daya selama pemindaian malware

Dalam peristiwa yang terkait dengan pemindaian malware, sumber daya EC2 tertentu dan volume EBS mungkin telah dilewati selama proses pemindaian. Tabel berikut mencantumkan alasan mengapa GuardDuty Malware Protection for EC2 mungkin tidak memindai sumber daya. Jika berlaku, gunakan langkah-langkah yang diusulkan untuk menyelesaikan masalah ini, dan pindai sumber daya ini saat berikutnya GuardDuty Malware Protection for EC2 memulai pemindaian malware. Masalah lainnya digunakan untuk memberi tahu Anda tentang jalannya peristiwa dan tidak dapat ditindaklanjuti.

Alasan untuk melewatkan	Penjelasan	Langkah-langkah yang diusulkan	
`RESOURCE_NOT_FOUND`	Yang `resourceArn` disediakan untuk memulai pemindaian malware sesuai permintaan tidak ditemukan di AWS lingkungan Anda.	Valid `resourceArn` asi instans Amazon EC2 atau beban kerja kontainer Anda, lalu coba lagi.	
`ACCOUNT_INELIGIBLE`	ID AWS akun tempat Anda mencoba memulai pemindaian On-demand malware belum diaktifkan GuardDuty.	Verifikasi GuardDuty apakah diaktifkan untuk AWS akun ini. Saat Anda mengaktifkan GuardDuty yang baru, mungkin Wilayah AWS perlu waktu hingga 20 menit untuk menyinkronkan.	
`UNSUPPORTED_KEY_ENCRYPTION`	GuardDuty Perlindungan Malware untuk EC2 mendukung volume yang tidak dienkripsi dan	Ganti kunci enkripsi Anda dengan kunci yang dikelola pelanggan. Untuk informasi selengkap	

Alasan untuk melewatkan	Penjelasan	Langkah-langkah yang diusulkan	
	dienkripsi dengan kunci yang dikelola pelanggan. Ini tidak mendukung pemindaian volume EBS yang dienkripsi menggunakan enkripsi Amazon EBS. Saat ini, ada perbedaan regional di mana alasan lewat ini tidak berlaku. Untuk informasi lebih lanjut tentang ini Wilayah AWS, lihatRegion-specific ketersediaan fitur.	nya tentang jenis enkripsi yang GuardDuty mendukung, lihatVolume Amazon EBS yang didukung untuk pemindaian malware.	

Alasan untuk melewatkan	Penjelasan	Langkah-langkah yang diusulkan	
`EXCLUDED_BY_SCAN_SETTINGS`	Instans EC2 atau volume EBS dikecualikan selama pemindaian malware. Ada dua kemungkinan - tag ditambahkan ke daftar inklusi tetapi sumber daya tidak terkait dengan tag ini, tag ditambahkan ke daftar pengecualian dan sumber daya dikaitkan dengan tag ini, atau tag disetel ke `true` untuk sumber daya ini. `GuardDutyExcluded`	Perbarui opsi pemindaian Anda atau tag yang terkait dengan sumber daya Amazon EC2 Anda. Untuk informasi selengkapnya, lihat Opsi pindai dengan tag yang ditentukan pengguna.	
`UNSUPPORTED_VOLUME_SIZE`	Volumenya lebih besar dari 2048 GB.	Tidak dapat ditindaklanjuti.	
`NO_VOLUMES_ATTACHED`	GuardDuty Perlindungan Malware untuk EC2 menemukan instance di akun Anda tetapi tidak ada volume EBS yang dilampirkan ke instance ini untuk melanjutkan pemindaian.	Tidak dapat ditindaklanjuti.	
`UNABLE_TO_SCAN`	Ini adalah kesalahan layanan internal.	Tidak dapat ditindaklanjuti.	

Alasan untuk melewatkan	Penjelasan	Langkah-langkah yang diusulkan	
SNAPSHOT_NOT_FOUND	Snapshot yang dibuat dari volume EBS dan dibagikan dengan akun layanan tidak ditemukan, dan Perlindungan GuardDuty Malware untuk EC2 tidak dapat melanjutkan pemindaian.	Periksa CloudTrail untuk memastikan bahwa snapshot tidak dihapus dengan sengaja.	
SNAPSHOT_QUOTA_REACHED	Anda telah mencapai volume maksimum yang diizinkan untuk snapshot untuk setiap Wilayah. Ini mencegah tidak hanya mempertahankan tetapi juga membuat snapshot baru.	Anda dapat menghapus snapshot lama atau meminta kenaikan kuota. Anda dapat melihat batas default untuk Snapshot per Wilayah dan cara meminta kenaikan kuota di bawah Kuota Layanan di Panduan Refer AWS ensi Umum.	

Alasan untuk melewatkan	Penjelasan	Langkah-langkah yang diusulkan	
`MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED`	Lebih dari 11 volume EBS dilampirkan ke instance EC2. GuardDuty Perlindungan Malware untuk EC2 memindai 11 volume EBS pertama, diperoleh dengan menyortir menurut abjad. `deviceName`	Tidak dapat ditindaklanjuti.	

Alasan untuk melewatkan	Penjelasan	Langkah-langkah yang diusulkan	
`UNSUPPORTED_PRODUCT_CODE_TYPE`	GuardDuty dapat memindai sebagian besar contoh dengan `productCode` as`marketplace` . Beberapa instans marketplace mungkin tidak memenuhi syarat untuk pemindaian. GuardDuty akan melewatkan contoh seperti itu dan mencatat alasannya sebagai`UNSUPPORTED_PRODUCT_CODE_TYPE` . Dukungan ini bervariasi di AWS GovCloud (US) dan Wilayah China. Untuk informasi selengkapnya, lihat Region-specific ketersediaan fitur. Untuk informasi selengkapnya, lihat AMI Ber bayar di Panduan Pengguna Amazon EC2. Untuk informasi tentang`productCode` , lihat ProductCo	Tidak dapat ditindaklanjuti.	

Alasan untuk melewatkan	Penjelasan	Langkah-langkah yang diusulkan	
	de di Refer ensi API Amazon EC2.		

Melaporkan positif palsu dalam Perlindungan Malware untuk EC2

GuardDuty Perlindungan Malware untuk pemindaian EC2 dapat mengidentifikasi file yang tidak berbahaya di instans Amazon EC2 atau beban kerja kontainer Anda sebagai berbahaya atau berbahaya. Untuk meningkatkan pengalaman Anda dengan Perlindungan Malware untuk EC2 dan GuardDuty layanan, Anda dapat melaporkan hasil positif palsu jika Anda yakin bahwa file yang diidentifikasi berbahaya atau berbahaya selama pemindaian sebenarnya tidak mengandung malware.

Untuk melaporkan hasil pemindaian malware Amazon EC2 sebagai positif palsu

Untuk memulai proses, hubungi Dukungan. Gunakan langkah-langkah berikut untuk memberikan detail tentang sumber daya yang dipindai:

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Pilih Pemindaian malware EC2.
3. Pilih pemindaian untuk melihat ID Temuannya.
4. Berikan ID Finding. Anda juga harus memberikan SHA-256 hash file. Ini diperlukan untuk memastikan bahwa Perlindungan GuardDuty Malware untuk EC2 telah menerima file yang benar.
5. Dukungan Tim akan memberi Anda URL presigned Amazon Simple Storage Service (Amazon S3) yang dapat Anda gunakan untuk mengunggah file dan hash yang berpotensi berbahaya. SHA-256 Untuk informasi tentang langkah-langkah untuk mengunggah objek yang dipindai, lihat Mengunggah objek dengan URL yang telah ditetapkan sebelumnya di Panduan Pengguna Amazon S3.
6. Setelah Anda mengunggah file, beri tahu Dukungan tim.

   Dukungan Akan memberikan pengakuan setelah menerima file. Anggota tim GuardDuty layanan akan menganalisis kiriman Anda, dan mengambil langkah-langkah yang tepat untuk meningkatkan pengalaman Anda dengan Perlindungan Malware untuk EC2 dan layanan.

GuardDuty Dukungan Tim akan terus memberikan pembaruan status pada kasus Anda. GuardDuty menyimpan objek S3 Anda selama tidak lebih dari 30 hari.

Melaporkan hasil pemindaian objek S3 sebagai positif palsu dalam Perlindungan Malware untuk S3

Perlindungan Malware untuk pemindaian S3 dapat mengidentifikasi objek sebagai berpotensi berbahaya atau berbahaya. Jika Anda yakin bahwa objek S3 yang ditunjukkan tidak mengandung malware, laporkan hasil pemindaian malware ini sebagai positif palsu.

Anda dapat mengirimkan laporan positif palsu bahkan ketika Anda menggunakan Perlindungan Malware untuk S3 secara independen. Dalam hal GuardDuty ini, tidak dirancang untuk menghasilkan temuan. Untuk informasi tentang memeriksa status pemindaian dan status hasil, lihatMemantau pemindaian objek S3.

Untuk melaporkan hasil pemindaian malware objek S3 sebagai positif palsu

Untuk memulai proses, hubungi Dukungan. Gunakan langkah-langkah berikut untuk memberikan detail tentang objek S3 yang dipindai:

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Tergantung pada kasus penggunaan Anda, pilih langkah-langkah yang sesuai:

   Using Malware Protection for S3 with GuardDuty

   1. Di panel navigasi, pilih Temuan.
   2. Pada halaman Temuan, pilih temuan positif palsu untuk melihat detailnya.
   3. Dengan memeriksa detail temuan, berikan Finding ID, Region, Nama bucket S3 yang dilindungi, dan Kunci objek yang dipindai.

      Dari detail jalur Item, berikan Hash objek. Ini diperlukan untuk memastikan bahwa GuardDuty telah menerima file yang benar.

   Using Malware Protection for S3 independently

   Berikan nama bucket S3 yang dilindungi, nama objek yang dipindai, dan. Wilayah AWS

3. Dukungan Tim akan memberi Anda URL presigned Amazon Simple Storage Service (Amazon S3) yang dapat Anda gunakan untuk mengunggah file dan hash yang berpotensi berbahaya. Untuk informasi tentang langkah-langkah untuk mengunggah objek yang dipindai, lihat Mengunggah objek dengan URL yang telah ditetapkan sebelumnya di Panduan Pengguna Amazon S3.
4. Setelah mengunggah objek S3, beri tahu tim. Dukungan

Surat Dukungan wasiat memberikan pengakuan menerima objek. Anggota tim GuardDuty layanan akan menganalisis kiriman Anda, dan mengambil langkah-langkah yang tepat untuk meningkatkan pengalaman Anda dengan Perlindungan Malware untuk S3 dan layanan. GuardDuty Dukungan Tim akan terus memberikan pembaruan status pada kasus Anda. GuardDuty menyimpan objek S3 Anda selama tidak lebih dari 30 hari.

Melaporkan positif palsu dalam Perlindungan Malware untuk Backup

Untuk meningkatkan pengalaman Anda dengan Perlindungan GuardDuty Malware untuk Pencadangan, Anda dapat melaporkan potensi positif palsu dan negatif palsu.

Untuk melaporkan potensi positif palsu atau negatif palsu yang diidentifikasi dalam Perlindungan Malware untuk Cadangan

Untuk memulai proses, hubungi Dukungan. Gunakan langkah-langkah berikut untuk memberikan detail tentang sumber daya yang dipindai:

1. Masuk ke Konsol Manajemen AWS dan buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Pilih Pemindaian Malware.
3. Pilih pemindaian untuk melihat ID Temuannya.
4. Berikan ID Finding. Anda juga harus memberikan SHA-256 hash file tersebut. Ini diperlukan untuk memastikan bahwa GuardDuty telah menerima file yang benar. Harap berikan juga wilayah tempat Anda akan memberikan sampelnya.
5. Dukungan Tim akan memberi Anda URL presigned Amazon Simple Storage Service (Amazon S3) yang akan Anda gunakan untuk mengunggah file dan hash yang berpotensi berbahaya. SHA-256 Untuk informasi tentang langkah-langkah untuk mengunggah sumber daya yang

dipindai, lihat Mengunggah objek dengan URL yang telah ditetapkan sebelumnya di Panduan Pengguna Amazon S3.

6. Setelah Anda mengunggah file, beri tahu Dukungan tim.

   Dukungan Akan memberikan pengakuan setelah menerima file. Anggota tim GuardDuty layanan akan menganalisis kiriman Anda, dan mengambil langkah-langkah yang tepat untuk meningkatkan pengalaman Anda dengan Perlindungan Malware untuk EC2. Dukungan Tim akan terus memberikan pembaruan status pada kasus Anda. GuardDuty menyimpan objek S3 Anda selama tidak lebih dari 30 hari.

Memperbaiki temuan GuardDuty keamanan yang terdeteksi

Amazon GuardDuty menghasilkan temuan yang menunjukkan temuan keamanan potensial yang terkait GuardDuty dengan deteksi ancaman dasar dan rencana perlindungan khusus. Bagian berikut menjelaskan langkah-langkah perbaikan yang disarankan untuk skenario ini. Jika ada skenario remediasi alternatif, mereka akan dijelaskan dalam deskripsi untuk setiap jenis temuan. Anda dapat mengakses informasi selengkapnya tentang tipe temuan dengan memilihnya dari tabel Tipe temuan aktif.

Daftar Isi

- Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan
- Memperbaiki bucket S3 yang berpotensi dikompromikan
- Memperbaiki objek S3 yang berpotensi berbahaya
- Memperbaiki Snapshot EBS yang berpotensi dikompromikan
- Memperbaiki AMI EC2 yang berpotensi dikompromikan
- Memperbaiki Titik Pemulihan EC2 yang berpotensi terganggu
- Memperbaiki Titik Pemulihan S3 yang berpotensi dikompromikan
- Memperbaiki cluster ECS yang berpotensi dikompromikan
- Memperbaiki potensi terganggu AWS credentials
- Memperbaiki wadah mandiri yang berpotensi dikompromikan
- Memperbaiki temuan Perlindungan EKS
- Memperbaiki temuan Pemantauan Runtime
- Memulihkan database yang berpotensi dikompromikan
- Memperbaiki fungsi Lambda yang berpotensi dikompromikan

Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan

Saat GuardDuty menghasilkan jenis temuan yang menunjukkan sumber daya Amazon EC2 yang berpotensi dikompromikan, maka Sumber Daya Anda akan menjadi Instans. Jenis temuan potensial bisa berupaTipe temuan EC2,GuardDuty Jenis penemuan Runtime Monitoring, atauPerlindungan Malware untuk jenis pencarian EC2. Jika perilaku yang menyebabkan temuan diharapkan di lingkungan Anda, maka pertimbangkan untuk menggunakannyaAturan penekanan.

Lakukan langkah-langkah berikut untuk memperbaiki instans Amazon EC2 yang berpotensi dikompromikan:

1. Mengidentifikasi instans Amazon EC2 yang berpotensi dikompromikan

   Selidiki instans yang berpotensi disusupi untuk malware dan menghapus malware yang ditemukan. Anda dapat menggunakannya On-demand pemindaian malware GuardDuty untuk mengidentifikasi malware di instans EC2 yang berpotensi dikompromikan, atau memeriksa AWS Marketplace untuk melihat apakah ada produk mitra yang bermanfaat untuk mengidentifikasi dan menghapus malware.

2. Isolasi instans Amazon EC2 yang berpotensi dikompromikan

   Jika memungkinkan, gunakan langkah-langkah berikut untuk mengisolasi instance yang berpotensi dikompromikan:

   1. Buat grup keamanan Isolasi khusus. Grup keamanan isolasi seharusnya hanya memiliki akses masuk dan keluar dari alamat IP tertentu. Pastikan tidak ada aturan masuk atau keluar yang mengizinkan lalu lintas. `0.0.0.0/0 (0-65535)`
   2. Kaitkan grup keamanan Isolasi dengan instance ini.
   3. Hapus semua asosiasi grup keamanan selain grup keamanan Isolasi yang baru dibuat dari instance yang berpotensi dikompromikan.

   > **Note**
   >
   > Koneksi yang dilacak yang ada tidak akan dihentikan sebagai akibat dari perubahan grup keamanan - hanya lalu lintas masa depan yang akan secara efektif diblokir oleh grup keamanan baru.
   > Untuk informasi tentang memblokir lalu lintas lebih lanjut dari koneksi yang ada yang mencurigakan, lihat Menegakkan NACL berdasarkan jaringan IoCs untuk mencegah lalu lintas lebih lanjut di Pedoman Respon Insiden.

3. Identifikasi sumber aktivitas yang mencurigakan

   Jika malware terdeteksi, maka berdasarkan jenis temuan di akun Anda, identifikasi dan hentikan aktivitas yang berpotensi tidak sah pada instans EC2 Anda. Ini mungkin memerlukan tindakan seperti menutup port terbuka, mengubah kebijakan akses, dan memutakhirkan aplikasi untuk memperbaiki kerentanan.

Jika Anda tidak dapat mengidentifikasi dan menghentikan aktivitas tidak sah pada instans EC2 yang berpotensi dikompromikan, sebaiknya hentikan instans EC2 yang disusupi dan menggantinya dengan instans baru sesuai kebutuhan. Berikut adalah sumber daya tambahan untuk mengamankan instans EC2 Anda:

- Bagian Keamanan dan Jaringan di Prakti k terbaik untuk Amazon EC2
- Grup keamanan Amazon EC2 untuk inst ans Linux.
- Keamanan di Amazon EC2
- Tips untuk mengamankan instans EC2 Anda (Linux).
- AWS praktik terbaik keamanan
- AWS Panduan Teknis Respons Insiden Keamanan.

4. Jelajahi AWS re:Post

   Telus AWS re:Post uri untuk bantuan lebih lanjut.

5. Kirim permintaan dukungan teknis

   Jika Anda adalah pelanggan paket dukungan premium, Anda dapat mengirimkan permintaan dukungan teknis.

Memperbaiki bucket S3 yang berpotensi dikompromikan

Saat GuardDuty dihasilkanGuardDuty Jenis temuan perlindungan S3, ini menunjukkan bahwa bucket Amazon S3 Anda telah dikompromikan. Jika perilaku yang menyebabkan temuan diharapkan di lingkungan Anda, maka pertimbangkan untuk membuatAturan penekanan. Jika perilaku ini tidak diharapkan, ikuti langkah-langkah yang disarankan ini untuk memperbaiki bucket Amazon S3 yang berpotensi terganggu di AWS lingkungan Anda:

1. Identifikasi sumber daya S3 yang berpotensi dikompromikan.

   Penem GuardDuty uan untuk S3 akan mencantumkan bucket S3 terkait, Nama Sumber Daya Amazon (ARN), dan pemiliknya dalam detail temuan.

2. Identifikasi sumber aktivitas mencurigakan dan panggilan API yang digunakan.

   Panggilan API yang digunakan akan terdaftar sebagai `API` dalam detail temuan. Sumbernya akan menjadi prinsipal IAM (baik peran IAM, pengguna, atau akun) dan detail identifikasi akan dicantumkan dalam temuan. Tergantung pada jenis sumbernya, alamat IP jarak jauh atau info

domain sumber akan tersedia dan dapat membantu Anda mengevaluasi apakah sumber tersebut diotorisasi. Jika temuan tersebut melibatkan kredenSIAL dari instans Amazon EC2, detail untuk sumber daya tersebut juga akan disertakan.

3. Tentukan apakah sumber panggilan diotorisasi untuk mengakses sumber daya yang diidentifikasi.

   Misalnya, pertimbangkan hal berikut:

   - Jika pengguna IAM terlibat, mungkinkah kredensialnya berpotensi dikompromikan? Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.
   - Jika API dipanggil dari prinipal yang sebelumnya tidak memiliki riwayat memanggil tipe API ini, apakah sumber ini memerlukan izin akses untuk operasi ini? Dapatkah izin bucket dibatasi secara lebih lanjut?
   - Jika akses terlihat dari nama pengguna `ANONYMOUS_PRINCIPAL` dengan tipe pengguna dari `AWSAccount`, ini menunjukkan bahwa bucket bersifat publik dan telah diakses. Haruskah bucket ini dibuat publik? Jika tidak, tinjau rekomendasi keamanan di bawah ini untuk solusi alternatif untuk berbagi sumber daya S3.
   - Jika akses terjadi karena `PreflightRequest` panggilan berhasil dilihat dari nama pengguna `ANONYMOUS_PRINCIPAL` dengan tipe pengguna, **`AWSAccount`** ini menunjukkan bucket memiliki kum pulan kebijakan berbagi sumber daya lintas asal (CORS). Haruskah bucket ini memiliki kebijakan CORS? Jika tidak, pastikan bucket tidak bersifat publik secara tidak sengaja dan tinjau rekomendasi keamanan di bawah ini untuk solusi alternatif untuk berbagi sumber daya S3. Untuk informasi selengkapnya tentang CORS lihat Menggunakan berbagi sumber daya lintas asal (CORS) di panduan pengguna S3.

4. Tentukan apakah bucket S3 berisi data sensitif.

   Gunakan Amazon Macie untuk menentukan apakah bucket S3 berisi data sensitif, seperti informasi identitas pribadi (PII), data keuangan, atau kredenSIAL. Jika penemuan data sensitif otomatis diaktifkan untuk akun Macie Anda, tinjau detail bucket S3 untuk mendapatkan pemahaman yang lebih baik tentang konten bucket S3 Anda. Jika fitur ini dinonaktifkan untuk akun Macie Anda, sebaiknya aktifkan fitur ini untuk mempercepat penilaian Anda. Atau, Anda dapat membuat dan menjalankan tugas penemuan data sensitif untuk memeriksa objek bucket S3 untuk data sensitif. Untuk informasi selengkapnya, lihat M enemukan data sensitif dengan Macie.

Jika akses diotorisasi, Anda dapat mengabaikan temuan tersebut. Kon https://console.aws.amazon.com/guardduty/ sol memungkinkan Anda mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Untuk informasi selengkapnya, lihat Aturan penindasan di GuardDuty.

Jika Anda menentukan bahwa data S3 Anda telah diekspos atau diakses oleh pihak yang tidak berwenang, tinjau rekomendasi keamanan S3 berikut untuk memperketat izin dan membatasi akses. Solusi perbaikan yang tepat akan bergantung pada kebutuhan lingkungan spesifik Anda.

Rekomendasi berdasarkan kebutuhan akses bucket S3 tertentu

Daftar berikut memberikan rekomendasi berdasarkan kebutuhan akses bucket Amazon S3 tertentu:

- Untuk cara terpusat membatasi akses publik ke penggunaan data S3 Anda, S3 memblokir akses publik. Setelan akses publik blokir dapat diaktifkan untuk titik akses, bucket, dan AWS Akun melalui empat pengaturan berbeda untuk mengontrol perincian akses. Untuk informasi selengkapnya, lihat Mem blokir setelan akses publik di Panduan Pengguna Amazon S3.
- AWS Kebijakan akses dapat digunakan untuk mengontrol bagaimana pengguna IAM dapat mengakses sumber daya Anda atau bagaimana bucket Anda dapat diakses. Untuk informasi selengkapnya, lihat Menggunakan kebijakan bucket dan kebijakan pengguna di Panduan Pengguna Amazon S3.

  Selain itu, Anda dapat menggunakan Titik Akhir Virtual Private Cloud (VPC) dengan kebijakan bucket S3 untuk membatasi akses ke titik akhir VPC tertentu. Untuk informasi selengkapnya, lihat Mengon trol akses dari titik akhir VPC dengan kebijakan bucket di Panduan Pengguna Amazon S3
- Untuk mengizinkan akses sementara ke objek S3 Anda ke entitas tepercaya di luar akun Anda, Anda dapat membuat URL yang ditandatangani sebelumnya melalui S3. Akses ini dibuat menggunakan kredensial akun Anda dan bergantung pada kredensial yang digunakan dapat bertahan 6 jam hingga 7 hari. Untuk informasi selengkapnya, lihat Menggunakan URL yang ditandatangani sebelumnya untuk mengunduh dan mengunggah objek di Panduan Pengguna Amazon S3.
- Untuk kasus penggunaan yang mengharuskan berbagi objek S3 antara sumber yang berbeda, Anda dapat menggunakan S3 Access Points untuk membuat set izin yang membatasi akses hanya untuk mereka yang berada dalam jaringan pribadi Anda. Untuk informasi selengkapnya, lihat M engelola akses ke kumpulan data bersama dengan titik akses di Panduan Pengguna Amazon S3.
- Untuk memberikan akses ke sumber daya S3 Anda dengan aman ke AWS Akun lain, Anda dapat menggunakan daftar kontrol akses (ACL), untuk informasi selengkapnya lihat ikhtisar daftar kontrol akses (ACL) di Panduan Pengguna Amazon S3.

Untuk informasi selengkapnya tentang opsi keamanan S3, lihat Praktik terbaik keamanan untuk Amazon S3 di Panduan Pengguna Amazon S3.

Memperbaiki objek S3 yang berpotensi berbahaya

Saat GuardDuty dihasilkanPerlindungan Malware untuk tipe pencarian S3, ini menunjukkan bahwa objek yang baru diunggah di bucket Amazon S3 Anda berisi malware. Jenis sumber daya adalah S3 Object.

Gunakan langkah-langkah yang disarankan berikut untuk berpotensi memperbaiki temuan yang dihasilkan:

1. Identifikasi objek S3 yang berpotensi berbahaya dengan memeriksa yang S3ObjectDetails terkait dengan temuan.
2. Isolasi objek S3 yang terkena dampak. Jika Anda telah mengaktifkan penandaan pada saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3 terkait, Anda GuardDuty harus menetapkan tag Ber bahaya ke objek ini. Gunakan kontrol akses berbasis tag (TBAC) untuk membatasi akses ke objek S3 ini. Untuk informasi selengkapnya, lihat Menggunakan kontrol akses berbasis tag (TBAC).

   Atau, jika Anda tidak memerlukan objek ini lagi, Anda juga dapat memilih untuk menghapusnya atau memindahkannya ke bucket S3 yang terisolasi. Untuk informasi tentang pertimbangan untuk menghapus objek S3, lihat Menghapus objek di Panduan Pengguna Amazon S3.

Memperbaiki Snapshot EBS yang berpotensi dikompromikan

Kapan GuardDuty menghasilkan Execution:EC2/MaliciousFile! Jenis penemuan snapshot, ini menunjukkan bahwa malware telah terdeteksi dalam snapshot Amazon EBS. Lakukan langkah-langkah berikut untuk memperbaiki snapshot yang berpotensi dikompromikan:

1. Identifikasi snapshot yang berpotensi dikompromikan

   1. Identifikasi snapshot yang berpotensi dikompromikan. Penem GuardDuty uan untuk snapshot EBS akan mencantumkan ID snapshot yang terpengaruh, Nama Sumber Daya Amazon (ARN), dan detail pemindaian malware terkait dalam detail temuan.
   2. Tinjau detail titik pemulihan menggunakan perintah berikut:

      ```
      aws backup describe-recovery-point –backup-vault-name 021345abcdef6789 –recovery-point-arn "arn:aws:ec2:us-east-1::snapshot/snap-abcdef01234567890"
      ```

2. Batasi akses snapshot yang dikompromikan

Tinjau dan ubah kebijakan akses brankas cadangan untuk membatasi akses titik pemulihan dan menangguhkan pekerjaan pemulihan otomatis yang mungkin menggunakan snapshot ini.

1. Tinjau izin berbagi saat ini:

```
aws ec2 describe-snapshot-attribute --snapshot-id snap-abcdef01234567890 --
attribute createVolumePermission
```

2. Hapus akses akun tertentu:

```
aws ec2 modify-snapshot-attribute --snapshot-id snap-abcdef01234567890 --
attribute createVolumePermission --operation-type remove --user-ids 111122223333
```

3. Untuk opsi CLI tambahan, lihat dokumentasi CLI modify-snapshot-atribut.

3. Ambil tindakan remediasi

- Sebelum melanjutkan penghapusan, pastikan Anda telah mengidentifikasi semua dependensi dan memiliki cadangan yang tepat jika diperlukan.

Memperbaiki AMI EC2 yang berpotensi dikompromikan

Kapan GuardDuty menghasilkan Execution:EC2/MaliciousFile! Jenis penemuan AMI, ini menunjukkan bahwa malware telah terdeteksi di Amazon Machine Image (AMI). Lakukan langkah-langkah berikut untuk memperbaiki AMI yang berpotensi dikompromikan:

1. Identifikasi AMI yang berpotensi dikompromikan

   1. Tem GuardDuty uan untuk AMI akan mencantumkan ID AMI yang terpengaruh, Nama Sumber Daya Amazon (ARN), dan detail pemindaian malware terkait dalam detail temuan.
   2. Tinjau gambar sumber AMI:

```
aws ec2 describe-images --image-ids ami-021345abcdef6789
```

2. Batasi akses ke sumber daya yang dikompromikan

   1. Tinjau dan ubah kebijakan akses brankas cadangan untuk membatasi akses titik pemulihan dan menangguhkan pekerjaan pemulihan otomatis yang mungkin menggunakan titik pemulihan ini.

2. Hapus Izin dari izin AMI sumber

   Pertama lihat izin yang ada:

   ```
   aws ec2 describe-image-attribute --image-id ami-abcdef01234567890 --attribute
    launchPermission
   ```

   Kemudian hapus izin individu:

   ```
   aws ec2 modify-image-attribute --image-id ami-abcdef01234567890 --launch-
   permission '{"Remove":[{"UserId":"111122223333"}]}'
   ```

   Untuk opsi CLI tambahan, lihat Berbagi AMI dengan akun tertentu - Amazon Elastic Compute Cloud

3. Jika sumbernya adalah Instans EC2, lihat: Memperbaiki instans Amazon EC 2 yang berpotensi dikompromikan.

3. Ambil tindakan remediasi

- Sebelum melanjutkan penghapusan, pastikan Anda telah mengidentifikasi semua dependensi dan memiliki cadangan yang tepat jika diperlukan.

Memperbaiki Titik Pemulihan EC2 yang berpotensi terganggu

Kapan GuardDuty menghasilkan Execution:EC2/MaliciousFile! RecoveryPoint menemukan jenis, ini menunjukkan bahwa malware telah terdeteksi di sumber daya Cadangan Titik Pemulihan EC2. Lakukan langkah-langkah berikut untuk memperbaiki titik pemulihan yang berpotensi terganggu:

1. Identifikasi Titik Pemulihan EC2 yang berpotensi terganggu

   1. Tem GuardDuty uan untuk EC2 Recovery Point akan mencantumkan Nama Sumber Daya Amazon (ARN), dan detail pemindaian malware terkait dalam detail temuan:

      ```
      aws backup describe-recovery-point --backup-vault-name 021345abcdef6789
       --recovery-point-arn "arn:aws:backup:us-east-1:111122223333:recovery-
      point:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      ```

   2. Tinjau detail pemulihan untuk mencari gambar sumber:

```
aws backup get-recovery-point-restore-metadata --backup-vault-
name 021345abcdef6789 --recovery-point-arn "arn:aws:backup:us-
east-1:111122223333:recovery-point:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

2. Batasi akses ke sumber daya yang dikompromikan

   - Tinjau dan ubah kebijakan akses brankas cadangan untuk membatasi akses titik pemulihan dan menangguhkan pekerjaan pemulihan otomatis yang mungkin menggunakan titik pemulihan ini. Jika lingkungan Anda menggunakan penandaan sumber daya, beri tag titik pemulihan dengan tepat untuk menunjukkan titik tersebut sedang diselidiki dan pertimbangkan untuk menjeda pencadangan terjadwal jika perlu.

     Contoh:

     ```
     aws backup tag-resource -–resource-arn arn:aws:backup:us-
     east-1:111122223333:recovery-point:a1b2c3d4-5678-90ab-cdef-
     EXAMPLE11111 -–tags Investigation=Malware,DoNotDelete=True
     ```

3. Ambil tindakan remediasi

   - Sebelum melanjutkan penghapusan, pastikan Anda telah mengidentifikasi semua dependensi dan memiliki cadangan yang tepat jika diperlukan.

Memperbaiki Titik Pemulihan S3 yang berpotensi dikompromikan

Kapan GuardDuty menghasilkan Execution:S3/MaliciousFile! RecoveryPoint menemukan jenis, ini menunjukkan bahwa malware telah terdeteksi di sumber daya Cadangan Titik Pemulihan S3. Lakukan langkah-langkah berikut untuk memperbaiki titik pemulihan yang berpotensi terganggu:

1. Mengidentifikasi Titik Pemulihan S3 yang berpotensi terganggu

   1. Penem GuardDuty uan untuk titik pemulihan S3 akan mencantumkan ARN titik pemulihan yang terpengaruh, nama brankas cadangan, dan detail pemindaian malware terkait dalam detail temuan.
   2. Tinjau detail titik pemulihan:

      ```
      aws backup describe-recovery-point --backup-vault-name 021345abcdef6789
       --recovery-point-arn arn:aws:backup:us-east-1:123456789012:recovery-
      point:abcdef01234567890
      ```

2. Batasi akses ke sumber daya yang dikompromikan

   - Tinjau dan ubah kebijakan akses brankas cadangan untuk membatasi akses titik pemulihan dan menangguhkan pekerjaan pemulihan otomatis yang mungkin menggunakan titik pemulihan ini. Jika lingkungan Anda menggunakan penandaan sumber daya, beri tag titik pemulihan dengan tepat untuk menunjukkan titik tersebut sedang diselidiki dan pertimbangkan untuk menjeda pencadangan terjadwal jika perlu.

     Contoh:

     ```
     aws backup tag-resource –resource-arn arn:aws:backup:us-
     east-1:111122223333:recovery-point:abcdef01234567890 –
     tags Investigation=Malware,DoNotDelete=True
     ```

     Untuk detail tambahan lihat: Referensi Per intah CLI tag-resource

3. Ambil tindakan remediasi

   - Sebelum melanjutkan penghapusan, pastikan Anda telah mengidentifikasi semua dependensi dan memiliki cadangan yang tepat jika diperlukan.

Memperbaiki cluster ECS yang berpotensi dikompromikan

Penemuan cluster ECS yang berpotensi dikompromikan menunjukkan aktivitas mencurigakan atau berbahaya telah terdeteksi dalam lingkungan Amazon ECS Anda. Ini bisa termasuk akses tidak sah, eksekusi malware, atau perilaku berbahaya lainnya yang membahayakan beban kerja kontainer Anda.

Ikuti langkah-langkah berikut untuk memperbaiki cluster Amazon ECS yang berpotensi dikompromikan:

1. Identifikasi cluster ECS yang berpotensi dikompromikan dan ancaman yang terdeteksi (temuan)

   Detail cluster ECS yang terkena dampak tercantum di panel rincian tem GuardDuty uan.

2. Evaluasi sumber threat/malware

   Periksa malware dalam gambar kontainer. Jika malware terdeteksi, tinjau gambar kontainer yang digunakan. Gunakan ListTasks untuk mengidentifikasi semua tugas berjalan lainnya yang menggunakan gambar yang sama yang berpotensi dikompromikan.

3. Isolasi tugas yang terkena dampak

   Hentikan ancaman dengan memblokir semua lalu lintas jaringan (masuk dan keluar) ke tugas yang terpengaruh. Isolasi jaringan ini membantu mencegah serangan yang sedang berlangsung dengan memotong semua koneksi ke tugas yang dikompromikan.

Catatan: Jika Anda menentukan temuan ini dipicu oleh expected/legitimate aktivitas di lingkungan Anda, Anda dapat mengatur aturan penindasan untuk mencegah temuan serupa muncul. Untuk informasi tambahan, lihat Aturan penindasan di GuardDuty.

Memperbaiki potensi terganggu AWS credentials

Saat dihasilkan GuardDuty Tipe temuan IAM, ini menunjukkan bahwa AWS kredenSIAL Anda telah dikompromikan. Jenis Sumber Daya yang berpotensi di kompromikan adalah AccessKey.

Untuk memperbaiki kredenSIAL yang berpotensi dikompromikan di AWS lingkungan Anda, lakukan langkah-langkah berikut:

1. Identifikasi entitas IAM yang berpotensi dikompromikan dan panggilan API yang digunakan.

   Panggilan API yang digunakan akan terdaftar sebagai `API` dalam detail temuan. Entitas IAM (baik peran atau pengguna IAM) dan informasi pengidentifikasinya akan dicantumkan di bagian Sumber Daya pada detail temuan. Tipe entitas IAM yang terlibat dapat ditentukan oleh bidang Tipe Pengguna, nama entitas IAM akan berada di bidang Nama pengguna. Tipe entitas IAM yang terlibat dalam temuan juga dapat ditentukan oleh Access key ID yang digunakan.

   Untuk kunci yang diawali dengan `AKIA`:

   Jenis kunci ini adalah kredensi jangka panjang yang dikelola pelanggan yang terkait dengan pengguna IAM atau. Pengguna root akun AWS Untuk informasi tentang mengelola kunci akses untuk pengguna IAM, lihat M engelola kunci akses untuk pengguna IAM.

   Untuk kunci yang diawali dengan `ASIA`:

   Tipe kunci ini adalah kredensial sementara jangka pendek yang dihasilkan oleh AWS Security Token Service. Kunci ini hanya ada untuk waktu yang singkat dan tidak dapat dilihat atau dikelola di Konsol AWS Manajemen. Peran IAM akan selalu menggunakan AWS STS kredenSIAL, tetapi mereka juga dapat dibuat untuk Pengguna IAM, untuk informasi selengkapnya AWS STS lihat IAM: KredenSIAL keamanan sementara.

Jika peran digunakan, bidang Nama pengguna akan menunjukkan nama dari peran yang digunakan. Anda dapat menentukan bagaimana kunci diminta AWS CloudTrail dengan memeriksa `sessionIssuer` elemen entri CloudTrail log, untuk informasi lebih lanjut lihat IAM dan AWS STS informasi di CloudTrail.

2. Tinjau izin untuk entitas IAM.

   Buka konsol IAM. Bergantung pada jenis entitas yang digunakan, pilih tab Pengguna atau Peran, dan temukan entitas yang terpengaruh dengan mengetikkan nama yang diidentifikasi ke bidang pencarian. Gunakan tab Izin dan Penasihat Akses untuk meninjau izin efektif untuk entitas tersebut.

3. Tentukan apakah kredentif entitas IAM digunakan secara sah.

   Hubungi pengguna kredensial untuk menentukan apakah aktivitas tersebut disengaja.

   Misalnya, cari tahu apakah pengguna melakukan hal berikut:

   - Memanggil operasi API yang tercantum dalam temuan GuardDuty
   - Memanggil operasi API pada saat yang tercantum dalam temuan GuardDuty
   - Memanggil operasi API dari alamat IP yang tercantum dalam temuan GuardDuty

Jika aktivitas ini merupakan penggunaan AWS kredenSIAL yang sah, Anda dapat mengabaikan tem GuardDuty uan tersebut. Kon https://console.aws.amazon.com/guardduty/ sol memungkinkan Anda mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Untuk informasi selengkapnya, lihat Aturan penindasan di GuardDuty.

Jika Anda tidak dapat mengonfirmasi apakah aktivitas ini merupakan penggunaan yang sah, itu bisa jadi akibat kompromi terhadap kunci akses tertentu - kredentif masuk pengguna IAM, atau mungkin keseluruhan. Akun AWS Jika Anda mencurigai kredensiran Anda telah dikompromikan, tinjau informasi di Informasi Saya Akun AWS mungkin dikompromikan untuk memperbaiki masalah ini.

Memperbaiki wadah mandiri yang berpotensi dikompromikan

Saat GuardDuty menghasilkan jenis temuan yang menunjukkan wadah yang berpotensi dikompromik an, jenis Resource Anda akan menjadi Container. Jika perilaku yang menyebabkan temuan diharapkan di lingkungan Anda, maka pertimbangkan untuk menggunakannyaAturan penekanan.

Untuk memperbaiki kredenSIAL yang berpotensi dikompromikan di AWS lingkungan Anda, lakukan langkah-langkah berikut:

1. Isolasi wadah yang berpotensi dikompromikan

   Langkah-langkah berikut akan membantu Anda mengidentifikasi beban kerja kontainer yang berpotensi berbahaya:

   - Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
   - Pada halaman Temuan, pilih temuan yang sesuai untuk melihat panel temuan.
   - Di panel temuan, di bawah bagian Sumber Daya yang terpengaruh, Anda dapat melihat ID dan Nama wadah.

   Isolasikan wadah ini dari beban kerja kontainer lainnya.

2. Jeda wadah

   Tangguhkan semua proses dalam wadah Anda.

   Untuk informasi tentang membekukan wadah Anda, lihat Menjeda wadah.

   Hentikan wadahnya.

   Jika langkah di atas gagal, dan wadah tidak berhenti, hentikan wadah agar tidak berjalan. Jika Anda telah mengaktifkan Retensi snapshot fitur ini, GuardDuty akan menyimpan snapshot volume EBS Anda yang berisi malware.

   Untuk informasi tentang menghentikan wadah, lihat Menghentikan wadah.

3. Mengevaluasi keberadaan malware

   Evaluasi apakah malware ada dalam gambar wadah.

Jika akses diotorisasi, Anda dapat mengabaikan temuan tersebut. Kon https://console.aws.amazon.com/guardduty/ sol memungkinkan Anda mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Kon GuardDuty sol memungkinkan Anda mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Lihat informasi yang lebih lengkap di Aturan penindasan di GuardDuty.

Memperbaiki temuan Perlindungan EKS

Amazon GuardDuty menghasilkan temuan yang menunjukkan potensi masalah keamanan Kubernetes saat Perlindungan EKS diaktifkan untuk akun Anda. Untuk informasi selengkapnya, lihat Perlindungan EKS. Bagian berikut menjelaskan langkah-langkah perbaikan yang disarankan untuk skenario ini. Tindakan remediasi spesifik dijelaskan dalam entri untuk jenis temuan tertentu. Anda dapat mengakses informasi selengkapnya tentang tipe temuan dengan memilihnya dari tabel Tipe temuan aktif.

Jika salah satu jenis temuan Perlindungan EKS dihasilkan dengan harapan, Anda dapat mempertimbangkan Aturan penindasan di GuardDuty untuk menambahkan untuk mencegah peringatan di masa mendatang.

Berbagai jenis serangan dan masalah konfigurasi dapat memicu temuan GuardDuty EKS Protection. Panduan ini membantu Anda mengidentifikasi akar penyebab GuardDuty temuan terhadap cluster Anda dan menguraikan panduan remediasi yang tepat. Berikut ini adalah akar penyebab utama yang mengarah pada temuan GuardDuty Kubernetes:

- Masalah konfigurasi potensial
- Memperbaiki pengguna Kubernetes yang berpotensi dikompromikan
- Memperbaiki pod Kubernetes yang berpotensi dikompromikan
- Memperbaiki node Kubernetes yang berpotensi terganggu
- Memperbaiki gambar kontainer yang berpotensi dikompromikan

> **Note**
>
> Sebelum Kubernetes versi 1.14, `system:unauthenticated` grup dikaitkan dengan dan secara `system:discovery` default. `system:basic-user` ClusterRoles Ini dapat memungkinkan akses yang tidak diinginkan dari pengguna anonim. Pembaruan cluster tidak mencabut izin ini, yang berarti bahwa meskipun Anda telah memperbarui cluster Anda ke versi 1.14 atau yang lebih baru, izin ini mungkin masih berlaku. Sebaiknya pisahkan izin ini dari `system:unauthenticated` grup.
> Untuk informasi selengkapnya tentang menghapus izin ini, lihat Mengam ankan cluster Amazon EKS dengan praktik terbaik di Panduan Pengguna Amazon EKS .

Masalah konfigurasi potensial

Jika temuan menunjukkan masalah konfigurasi, lihat bagian remediasi dari temuan tersebut untuk panduan penyelesaian masalah tertentu. Untuk informasi selengkapnya, lihat jenis temuan berikut yang menunjukkan masalah konfigurasi:

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- Setiap temuan yang berakhir pada SuccessfulAnonymousAccess

Memperbaiki pengguna Kubernetes yang berpotensi dikompromikan

Tem GuardDuty uan dapat menunjukkan pengguna Kubernetes yang dikompromikan ketika pengguna yang diidentifikasi dalam temuan telah melakukan tindakan API yang tidak terduga. Anda dapat mengidentifikasi pengguna di bagian detail pengguna Kubernetes dari detail pencarian di konsol, atau di JSON `resource.kubernetesDetails.kubernetesUserDetails` temuan. Rincian pengguna ini termasuk `user name` `uid`,, dan grup Kubernetes yang dimiliki pengguna.

Jika pengguna mengakses beban kerja menggunakan entitas IAM, Anda dapat menggunakan `Access Key details` bagian tersebut untuk mengidentifikasi detail peran atau pengguna IAM. Lihat jenis pengguna berikut dan panduan remediasinya.

> **Note**
>
> Anda dapat menggunakan Amazon Detective untuk menyelidiki lebih lanjut peran IAM atau pengguna yang diidentifikasi dalam temuan. Saat melihat detail temuan di GuardDuty konsol, pilih Investig ate in Detective. Kemudian pilih AWS pengguna atau peran dari item yang terdaftar untuk menyelidikinya di Detective.

Built-in Kubernetes admin — Pengguna default yang ditugaskan oleh Amazon EKS ke identitas IAM yang membuat cluster. Jenis pengguna ini diidentifikasi oleh nama penggunakubernetes-admin.

Untuk mencabut akses admin Kubernetes bawaan:

- Identifikasi `userType` dari `Access Key details` bagian tersebut.
  - Jika `userType` adalah Peran dan peran milik peran instans EC2:
    - Identifikasi contoh itu lalu ikuti instruksi diMemperbaiki instans Amazon EC2 yang berpotensi dikompromikan.
  - Jika `userType` adalah Pengguna, atau merupakan Peran yang diasumsikan oleh pengguna:
    1. Putar kunci akses pengguna itu.
    2. Putar rahasia apa pun yang dapat diakses pengguna.
    3. Tinjau informasi di My Akun AWS mungkin dikompromikan untuk detail lebih lanjut.

Pengguna terautentikasi OIDC — Pengguna yang diberikan akses melalui penyedia OIDC. Biasanya pengguna OIDC memiliki alamat email sebagai nama pengguna. Anda dapat memeriksa apakah cluster Anda menggunakan OIDC dengan perintah berikut: `aws eks list-identity-provider-configs --cluster-name` *`your-cluster-name`*

Untuk mencabut akses pengguna yang diautentikasi OIDC:

1. Putar kredenSIAL pengguna tersebut di penyedia OIDC.
2. Putar rahasia apa pun yang dapat diakses pengguna.

AWS-Auth ConfigMap defined user — Pengguna IAM yang diberikan akses melalui -auth. AWS ConfigMap Untuk informasi selengkapnya, lihat Mengelola pengguna atau IAM role untuk klaster Anda di Panduan Pengguna Amazon EKS. Anda dapat meninjau izin mereka menggunakan perintah berikut: `kubectl edit configmaps aws-auth --namespace kube-system`

Untuk mencabut akses AWS ConfigMap pengguna:

1. Gunakan perintah berikut untuk membuka ConfigMap.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifikasi peran atau entri pengguna di bawah bagian MaProles atau MapUsers dengan nama pengguna yang sama seperti yang dilaporkan di bagian detail pengguna Kubernetes dari temuan Anda. GuardDuty Lihat contoh berikut, di mana pengguna admin telah diidentifikasi dalam temuan.

```
apiVersion: v1
data:
  mapRoles: |
```

```
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. Hapus pengguna itu dari ConfigMap. Lihat contoh berikut di mana pengguna admin telah dihapus.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

4. Jika `userType` adalah Pengguna, atau merupakan Peran yang diasumsikan oleh pengguna:

   a. Putar kunci akses pengguna itu.

   b. Putar rahasia apa pun yang dapat diakses pengguna.

   c. Tinjau informasi di AWS Akun saya dapat dikompromikan untuk detail lebih lanjut.

Jika temuan tidak memiliki `resource.accessKeyDetails` bagian, pengguna adalah akun layanan Kubernetes.

Akun layanan — Akun layanan memberikan identitas untuk pod dan dapat diidentifikasi dengan nama pengguna dengan format berikut:`system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Untuk mencabut akses ke akun layanan:

1. Putar kredenSIAL akun layanan.
2. Tinjau panduan untuk kompromi pod di bagian berikut.

Memperbaiki pod Kubernetes yang berpotensi dikompromikan

Saat GuardDuty menentukan detail sumber daya pod atau beban kerja di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails` bagian, pod atau sumber daya beban kerja tersebut berpotensi dikompromikan. Tem GuardDuty uan dapat menunjukkan satu pod telah dikompromikan atau bahwa beberapa pod telah dikompromikan melalui sumber daya tingkat yang lebih tinggi. Lihat skenario kompromi berikut untuk panduan tentang cara mengidentifikasi pod atau pod yang telah disusupi.

Kompromi pod tunggal

Jika `type` bidang di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails` bagian adalah pod, temuan mengidentifikasi satu pod. Bidang nama adalah `name` dari pod dan `namespace` bidang adalah namespace nya.

Untuk informasi tentang mengidentifikasi node pekerja yang menjalankan pod, lihat Men gidentifikasi pod yang melanggar dan node pekerja di Panduan Prakti k Terbaik Amazon EKS.

Pod dikompromikan melalui sumber daya beban kerja

Jika `type` bidang di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails` bagian mengidentifikasi Sumber Daya Beb an Kerja, seperti a`Deployment`, kemungkinan semua pod dalam sumber daya beban kerja tersebut telah dikompromikan.

Untuk informasi tentang mengidentifikasi semua pod sumber daya beban kerja dan node tempat mereka berjalan, lihat Mengi dentifikasi pod yang melanggar dan node pekerja menggunakan nama beban kerja di Panduan Prakti k Terbaik Amazon EKS.

Pod dikompromikan melalui akun layanan

Jika tem GuardDuty uan mengidentifikasi Akun Layanan di `resource.kubernetesDetails.kubernetesUserDetails` bagian tersebut, kemungkinan pod yang menggunakan akun layanan yang diidentifikasi dikompromikan.

Nama pengguna yang dilaporkan oleh temuan adalah akun layanan jika memiliki format berikut:`system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Untuk informasi tentang mengidentifikasi semua pod menggunakan akun layanan dan node tempat mereka berjalan, lihat Mengi dentifikasi pod dan node pekerja yang melanggar menggunakan nama akun layanan di Panduan Prakti k Terbaik Amazon EKS.

Setelah mengidentifikasi semua pod yang dikompromikan dan node tempat mereka berjalan, lihat Meng isolasi pod dengan membuat kebijakan jaringan yang menolak semua lalu lintas masuk dan keluar ke pod di Panduan Prakti k Terbaik Amazon EKS.

Untuk memperbaiki pod yang berpotensi dikompromikan:

1. Identifikasi kerentanan yang membahayakan pod.
2. Terapkan perbaikan untuk kerentanan itu dan mulai pod pengganti baru.
3. Hapus pod yang rentan.

   Untuk informasi selengkapnya, lihat Men yebarkan kembali pod yang dikompromikan atau sumber daya beban kerja di Panduan Praktik Terbaik Amazon EKS.

Jika node pekerja telah diberi peran IAM yang memungkinkan Pod mendapatkan akses ke AWS sumber daya lain, hapus peran tersebut dari instans untuk mencegah kerusakan lebih lanjut dari serangan. Demikian pula, jika Pod telah ditetapkan peran IAM, evaluasi apakah Anda dapat menghapus kebijakan IAM dengan aman dari peran tersebut tanpa memengaruhi beban kerja lainnya.

Memperbaiki gambar kontainer yang berpotensi dikompromikan

Ketika tem GuardDuty uan menunjukkan kompromi pod, gambar yang digunakan untuk meluncurkan pod dapat berpotensi berbahaya atau dikompromikan. GuardDuty temuan mengidentifikasi gambar wadah di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` lapangan. Anda dapat menentukan apakah gambar itu berbahaya dengan memindai malware.

Untuk memperbaiki gambar kontainer yang berpotensi dikompromikan:

1. Berhenti menggunakan gambar segera dan hapus dari repositori gambar Anda.
2. Identifikasi semua pod menggunakan gambar yang berpotensi dikompromikan.

Untuk informasi selengkapnya, lihat Mengidentifikasi pod dengan gambar dan node pekerja yang rentan atau terganggu di Panduan Praktik Terbaik Amazon EKS.

3. Isolasi pod yang berpotensi dikompromikan, putar kredenSIAL, dan kumpulkan data untuk dianalisis. Untuk informasi selengkapnya, lihat Meng isolasi pod dengan membuat kebijakan jaringan yang menolak semua lalu lintas masuk dan keluar ke pod di Panduan Prakti k Terbaik Amazon EKS.
4. Hapus semua pod menggunakan gambar yang berpotensi dikompromikan.

Memperbaiki node Kubernetes yang berpotensi terganggu

Sebuah GuardDuty temuan dapat menunjukkan kompromi node jika pengguna yang diidentifikasi dalam temuan mewakili identitas node atau jika temuan menunjukkan penggunaan wadah istimewa.

Identitas pengguna adalah node pekerja jika bidang nama pengguna memiliki format berikut:`system:node:node name`. Misalnya, `system:node:ip-192-168-3-201.ec2.internal`. Ini menunjukkan bahwa musuh telah memperoleh akses ke node dan menggunakan kredenSIAL node untuk berbicara dengan titik akhir API Kubernetes.

Temuan menunjukkan penggunaan wadah istimewa jika satu atau lebih wadah yang tercantum dalam temuan memiliki bidang tem `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` uan yang disetel ke`True`.

Untuk memperbaiki node yang berpotensi dikompromikan:

1. Isolasi pod, putar kredensialnya, dan kumpulkan data untuk analisis forensik.

   Untuk informasi selengkapnya, lihat Meng isolasi pod dengan membuat kebijakan jaringan yang menolak semua lalu lintas masuk dan keluar ke pod di Panduan Prakti k Terbaik Amazon EKS.
2. Identifikasi akun layanan yang digunakan oleh semua pod yang berjalan pada node yang berpotensi dikompromikan. Tinjau izin mereka dan putar akun layanan jika diperlukan.
3. Hentikan node yang berpotensi dikompromikan.

Memperbaiki temuan Pemantauan Runtime

Saat Anda mengaktifkan Runtime Monitoring untuk akun Anda, Amazon GuardDuty dapat menghasilkan GuardDuty Jenis penemuan Runtime Monitoring yang menunjukkan potensi masalah keamanan di AWS lingkungan Anda. Masalah keamanan potensial menunjukkan instans Amazon EC2 yang dikompromikan, beban kerja kontainer, cluster Amazon EKS, atau serangkaian kredenSIAL yang dikompromikan di AWS lingkungan Anda. Agen keamanan memantau peristiwa runtime dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat jenis Sumber daya di detail temuan yang dihasilkan di GuardDuty konsol. Bagian berikut menjelaskan langkah-langkah remediasi yang disarankan untuk setiap jenis sumber daya.

Instance

Jika tipe Resource dalam rincian temuan adalah Instance, ini menunjukkan bahwa instans EC2 atau node EKS berpotensi dikompromikan.

- Untuk memperbaiki node EKS yang dikompromikan, lihatMemperbaiki node Kubernetes yang berpotensi terganggu.
- Untuk memperbaiki instans EC2 yang dikompromikan, lihat. Memperbaiki instans Amazon EC2 yang berpotensi dikompromikan

EKSCluster

Jika tipe Resource dalam detail temuan adalah EKSCluster, ini menunjukkan bahwa pod atau wadah di dalam cluster EKS berpotensi dikompromikan.

- Untuk memperbaiki pod yang dikompromikan, lihatMemperbaiki pod Kubernetes yang berpotensi dikompromikan.
- Untuk memperbaiki gambar kontainer yang dikompromikan, lihatMemperbaiki gambar kontainer yang berpotensi dikompromikan.

ECSCluster

Jika tipe Sumber daya dalam detail temuan adalah ECSCluster, ini menunjukkan bahwa tugas ECS atau wadah di dalam tugas ECS berpotensi dikompromikan.

1. Identifikasi cluster ECS yang terpengaruh

Temuan GuardDuty Runtime Monitoring memberikan detail cluster ECS di panel detail temuan atau di `resource.ecsClusterDetails` bagian dalam JSON temuan.

2. Identifikasi tugas ECS yang terpengaruh

   Temuan GuardDuty Runtime Monitoring memberikan detail tugas ECS di panel detail temuan atau di `resource.ecsClusterDetails.taskDetails` bagian dalam JSON pencarian.

3. Isolasikan tugas yang terpengaruh

   Isolasi tugas yang terkena dampak dengan menolak semua lalu lintas masuk dan keluar ke tugas. Aturan tolak semua lalu lintas dapat membantu menghentikan serangan yang sudah berlangsung, dengan memutuskan semua koneksi ke tugas.

4. Memperbaiki tugas yang dikompromikan
   a. Identifikasi kerentanan yang membahayakan tugas.
   b. Terapkan perbaikan untuk kerentanan itu dan mulai tugas penggantian baru.
   c. Hentikan tugas yang rentan.

Container

Jika tipe Resource dalam rincian temuan adalah Con tainer, ini menunjukkan bahwa wadah mandiri berpotensi dikompromikan.

- Untuk memperbaiki, lihatMemperbaiki wadah mandiri yang berpotensi dikompromikan.
- Jika temuan dihasilkan di beberapa wadah menggunakan gambar wadah yang sama, lihatMemperbaiki gambar kontainer yang berpotensi dikompromikan.
- Jika kontainer telah mengakses host EC2 yang mendasarinya, kredenSIAL instans terkaitnya mungkin telah dikompromikan. Untuk informasi selengkapnya, lihat Memperbaiki potensi terganggu AWS credentials.
- Jika aktor yang berpotensi berbahaya telah mengakses node EKS yang mendasarinya atau instans EC2, lihat remediasi yang disarankan di bawah tab EKSClu ster dan Instance.

Memperbaiki gambar kontainer yang dikompromikan

Ketika tem GuardDuty uan menunjukkan kompromi tugas, gambar yang digunakan untuk meluncurkan tugas dapat berbahaya atau dikompromikan. GuardDuty temuan mengidentifikasi gambar wadah di dalam `resource.ecsClusterDetails.taskDetails.containers.image`

lapangan. Anda dapat menentukan apakah gambar itu berbahaya atau tidak dengan memindai malware.

Untuk memperbaiki gambar kontainer yang dikompromikan

1. Berhenti menggunakan gambar segera dan hapus dari repositori gambar Anda.
2. Identifikasi semua tugas yang menggunakan gambar ini.
3. Hentikan semua tugas yang menggunakan gambar yang dikompromikan. Perbarui definisi tugas mereka sehingga mereka berhenti menggunakan gambar yang dikompromikan.

Memulihkan database yang berpotensi dikompromikan

GuardDuty menghasilkan Jenis temuan Perlindungan RDS yang menunjukkan perilaku login yang berpotensi mencurigakan dan anomali di Anda Basis data yang didukung setelah Anda mengaktifkan. Perlindungan RDS Menggunakan aktivitas login RDS, GuardDuty analisis dan profil ancaman dengan mengidentifikasi pola yang tidak biasa dalam upaya login.

> **Note**
>
> Anda dapat mengakses informasi lengkap tentang jenis temuan dengan memilihnya dari fileGuardDuty jenis temuan aktif.

Ikuti langkah-langkah yang disarankan ini untuk memulihkan database Amazon Aurora yang berpotensi dikompromikan di lingkungan Anda. AWS

Topik

- Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil
- Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal
- Memulihkan database yang berpotensi dikompromikan dengan aktivitas eksfiltrasi anomali
- Memulihkan database yang berpotensi dikompromikan dengan aktivitas destruktif anomali
- Memulihkan kredensi yang berpotensi dikompromikan
- Batasi akses jaringan

Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil

Langkah-langkah yang disarankan berikut dapat membantu Anda memulihkan database Aurora yang berpotensi dikompromikan yang menunjukkan perilaku tidak biasa terkait dengan peristiwa login yang berhasil.

1. Identifikasi database dan pengguna yang terpengaruh.

   GuardDuty Temuan yang dihasilkan memberikan nama database yang terpengaruh dan detail pengguna yang sesuai. Untuk informasi selengkapnya, lihat Detail temuan.

2. Konfirmasikan apakah perilaku ini diharapkan atau tidak terduga.

   Daftar berikut menentukan skenario potensial yang mungkin menyebabkan GuardDuty untuk menghasilkan temuan:

   - Seorang pengguna yang masuk ke database mereka setelah waktu yang lama berlalu.
   - Seorang pengguna yang login ke database mereka sesekali, misalnya, seorang analis keuangan yang log di setiap kuartal.
   - Aktor yang berpotensi mencurigakan yang terlibat dalam upaya login yang berhasil berpotensi membahayakan database.

3. Mulailah langkah ini jika perilakunya tidak terduga.

   1. Batasi akses basis data

      Batasi akses database untuk akun yang dicurigai dan sumber aktivitas login ini. Untuk informasi selengkapnya, lihat Memulihkan kredensi yang berpotensi dikompromikan dan Batasi akses jaringan.

   2. Menilai dampak dan menentukan informasi apa yang diakses.

      - Jika tersedia, tinjau log audit untuk mengidentifikasi potongan-potongan informasi yang mungkin telah diakses. Untuk informasi selengkapnya, lihat Memantau peristiwa, log, dan aliran di klaster DB Amazon Aurora di Panduan Pengguna Amazon Aurora.
      - Tentukan apakah ada informasi sensitif atau dilindungi yang diakses atau dimodifikasi.

Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal

Langkah-langkah yang disarankan berikut dapat membantu Anda memulihkan database Aurora yang berpotensi dikompromikan yang menunjukkan perilaku yang tidak biasa terkait dengan peristiwa login yang gagal.

1. Identifikasi database dan pengguna yang terpengaruh.

   GuardDuty Temuan yang dihasilkan memberikan nama database yang terpengaruh dan detail pengguna yang sesuai. Untuk informasi selengkapnya, lihat Detail temuan.

2. Identifikasi sumber upaya login yang gagal.

   GuardDuty Temuan yang dihasilkan menyediakan alamat IP dan organisasi ASN (jika itu adalah koneksi publik) di bawah bagian Aktor dari panel pencarian.

   Autonomous System (AS) adalah sekelompok satu atau lebih awalan IP (daftar alamat IP yang dapat diakses pada jaringan) yang dijalankan oleh satu atau lebih operator jaringan yang mempertahankan kebijakan routing tunggal yang didefinisikan dengan jelas. Operator jaringan membutuhkan Autonomous System Numbers (ASN) untuk mengontrol routing dalam jaringan mereka dan untuk bertukar informasi routing dengan penyedia layanan internet (ISP) lainnya.

3. Konfirmasikan bahwa perilaku ini tidak terduga.

   Periksa apakah aktivitas ini merupakan upaya untuk mendapatkan akses tidak sah tambahan ke database sebagai berikut:

   - Jika sumbernya internal, periksa apakah aplikasi salah konfigurasi dan coba koneksi berulang kali.
   - Jika ini adalah aktor eksternal, periksa apakah database yang sesuai menghadap publik atau salah konfigurasi dan dengan demikian memungkinkan pelaku jahat potensial untuk secara kasar memaksa nama pengguna umum.

4. Mulailah langkah ini jika perilakunya tidak terduga.

   1. Batasi akses basis data

      Batasi akses database untuk akun yang dicurigai dan sumber aktivitas login ini. Untuk informasi selengkapnya, lihat Memulihkan kredensi yang berpotensi dikompromikan dan Batasi akses jaringan.

2. Lakukan analisis akar penyebab dan tentukan langkah-langkah yang berpotensi menyebabkan aktivitas ini.

   Siapkan peringatan untuk mendapatkan pemberitahuan saat aktivitas mengubah kebijakan jaringan dan membuat status tidak aman. Untuk informasi selengkapnya, lihat Kebijakan Firewall AWS Network Firewall di Panduan AWS Network Firewall Pengembang.

Memulihkan database yang berpotensi dikompromikan dengan aktivitas eksfiltrasi anomali

Langkah-langkah yang direkomendasikan berikut dapat membantu Anda memulihkan database Aurora yang berpotensi dikompromikan yang menunjukkan perilaku tidak biasa terkait dengan peristiwa eksfiltrasi data.

1. Identifikasi database dan pengguna yang terpengaruh.

   GuardDuty Temuan yang dihasilkan memberikan nama database yang terpengaruh dan detail pengguna yang sesuai. Untuk informasi selengkapnya, lihat Detail temuan.

2. Identifikasi ruang lingkup data yang diakses.

   Tinjau log aktivitas data RDS yang tersedia untuk menentukan tabel dan baris mana yang diakses oleh pengguna anomali selama jendela waktu yang ditunjukkan oleh temuan. Menilai sensitivitas data yang berpotensi diekstraksi.

3. Konfirmasikan bahwa perilaku ini tidak terduga.

   Periksa apakah kegiatan ini mewakili perilaku operasional yang sah sebagai berikut:

   - Jika sumbernya internal, periksa apakah pekerjaan ETL terjadwal, alat pelaporan, atau proses pencadangan dapat menjelaskan volume kueri yang meningkat.
   - Jika ini adalah aktor eksternal atau atribut database yang sebelumnya tidak terlihat, periksa apakah kredensyal database yang sesuai mungkin telah diekspos atau dibagikan secara eksternal.
   - Tinjau apakah kombinasi volume dan atribut yang tidak terlihat (alamat IP, ASN, nama aplikasi) sejalan dengan perubahan operasional yang diketahui.

4. Mulailah langkah ini jika perilakunya tidak terduga.

   Cabut akses dan putar kredensil.

Segera ubah kata sandi pengguna database yang terpengaruh dan cabut sesi aktif. Jika pengguna memiliki hak istimewa yang tinggi, batasi sementara izin mereka untuk hanya-baca atau hapus akses sepenuhnya sampai penyelidikan selesai.

5. Menilai dampak bisnis.

   Identifikasi data yang dapat diakses oleh pengguna yang terpengaruh, tentukan apakah ada data sensitif atau teregulasi (PII, keuangan, layanan kesehatan) yang berpotensi diekstraksi, dan ikuti prosedur pemberitahuan pelanggaran data organisasi Anda jika berlaku.

6. Batasi akses jaringan.

   Batasi akses database untuk akun yang dicurigai dan sumber aktivitas ini. Tempatkan database di VPC pribadi jika belum dikonfigurasi, dan batasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat Batasi akses jaringan.

7. Lakukan analisis akar penyebab dan tentukan langkah-langkah yang berpotensi menyebabkan aktivitas ini.

   Siapkan peringatan untuk mendapatkan pemberitahuan saat aktivitas mengubah kebijakan jaringan dan membuat status tidak aman. Untuk informasi selengkapnya, lihat Kebijakan Firewall AWS Network Firewall di Panduan AWS Network Firewall Pengembang.

Memulihkan database yang berpotensi dikompromikan dengan aktivitas destruktif anomali

Langkah-langkah yang disarankan berikut dapat membantu Anda memulihkan database Aurora yang berpotensi dikompromikan yang menunjukkan perilaku tidak biasa yang terkait dengan destruktif atau peristiwa. `DELETE` `DROP`

1. Identifikasi database dan pengguna yang terpengaruh.

   GuardDuty Temuan yang dihasilkan memberikan nama database yang terpengaruh dan detail pengguna yang sesuai. Untuk informasi selengkapnya, lihat Detail temuan.

2. Identifikasi ruang lingkup operasi destruktif.

   Tinjau log aktivitas data RDS yang tersedia untuk menentukan tabel, baris, atau objek database mana yang dihapus atau dijatuhkan oleh pengguna anomali selama jendela waktu yang

ditunjukkan oleh temuan. Tentukan apakah kehilangan data dapat dipulihkan dari cadangan atau snapshot yang ada.

3. Konfirmasikan bahwa perilaku ini tidak terduga.

   Periksa apakah kegiatan ini mewakili perilaku operasional yang sah sebagai berikut:

   - Jika sumbernya internal, periksa apakah pekerjaan pemeliharaan terjadwal, skrip pembersihan, atau proses migrasi dapat menjelaskan `DELETE` atau `DROP` operasi.
   - Jika ini adalah aktor eksternal atau atribut database yang sebelumnya tidak terlihat, periksa apakah kredensyal database yang sesuai mungkin telah diekspos atau dikompromikan.
   - Tinjau apakah kombinasi operasi destruktif dan atribut yang tidak terlihat (alamat IP, ASN, nama aplikasi) sejalan dengan perubahan operasional yang diketahui.

4. Mulailah langkah ini jika perilakunya tidak terduga.

   Cabut akses dan putar kredensil.

   Segera ubah kata sandi pengguna database yang terpengaruh dan cabut sesi aktif. Hapus hak pengguna `DROP` dan `DELETE` hak istimewa sampai penyelidikan selesai untuk mencegah kerusakan data lebih lanjut.

5. Memulai pemulihan data.

   Jika kehilangan data dikonfirmasi, mulailah pemulihan point-in-time dari pencadangan otomatis atau pulihkan dari snapshot terbaru. Untuk Amazon Aurora, Anda dapat menggunakan backtrack untuk memundurkan database ke waktu sebelum aktivitas destruktif terjadi. Untuk Amazon RDS, gunakan pemulihan point-in-time untuk memulihkan ke titik sebelum acara.

6. Batasi akses jaringan dan perkeras izin.

   Batasi akses database untuk akun yang dicurigai dan sumber aktivitas ini. Tempatkan database di VPC pribadi jika belum dikonfigurasi, dan batasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Tinjau kebijakan IAM dan hak istimewa pengguna database untuk menerapkan akses hak istimewa paling sedikit, dan aktifkan perlindungan penghapusan pada instans RDS jika belum diaktifkan. Untuk informasi selengkapnya, lihat Batasi akses jaringan.

7. Lakukan analisis akar penyebab dan tentukan langkah-langkah yang berpotensi menyebabkan aktivitas ini.

Siapkan peringatan untuk mendapatkan pemberitahuan saat aktivitas mengubah kebijakan jaringan dan membuat status tidak aman. Untuk informasi selengkapnya, lihat Kebijakan Firewall AWS Network Firewall di Panduan AWS Network Firewall Pengembang.

Memulihkan kredensi yang berpotensi dikompromikan

GuardDuty Temuan dapat menunjukkan bahwa kredensyal pengguna untuk database yang terpengaruh telah dikompromikan ketika pengguna yang diidentifikasi dalam temuan telah melakukan operasi database yang tidak terduga. Anda dapat mengidentifikasi pengguna di bagian detail pengguna RDS DB dalam panel pencarian di konsol, atau di `resource.rdsDbUserDetails` dalam temuan JSON. Detail pengguna ini termasuk nama pengguna, aplikasi yang digunakan, database diakses, versi SSL, dan metode otentikasi.

- Untuk mencabut akses atau memutar kata sandi untuk pengguna tertentu yang terlibat dalam temuan, lihat Keamanan dengan Amazon Aurora MySQL, atau Keamanan dengan Amazon Aurora PostgreSQL di Panduan Pengguna Amazon Aurora.
- Gunakan AWS Secrets Manager untuk menyimpan dengan aman dan secara otomatis memutar rahasia untuk database Amazon Relational Database Service (RDS). Untuk informasi selengkapnya, lihat AWS Secrets Manager tutorial di Panduan AWS Secrets Manager Pengguna.
- Gunakan autentikasi basis data IAM untuk mengelola akses pengguna database tanpa perlu kata sandi. Untuk informasi selengkapnya, lihat autentikasi database IAM di Panduan Pengguna Amazon Aurora.

  Untuk informasi selengkapnya, lihat Praktik terbaik keamanan untuk Amazon Relational Database Service di Panduan Pengguna Amazon RDS.

Batasi akses jaringan

GuardDuty Temuan mungkin menunjukkan bahwa database dapat diakses di luar aplikasi Anda, atau Virtual Private Cloud (VPC). Jika alamat IP jarak jauh dalam temuan adalah sumber koneksi yang tidak terduga, audit grup keamanan. Daftar grup keamanan yang dilampirkan ke database tersedia di bawah Grup keamanan di https://console.aws.amazon.com/rds/konsol, atau di `resource.rdsDbInstanceDetails.dbSecurityGroups` temuan JSON. Untuk informasi selengkapnya tentang mengonfigurasi grup keamanan, lihat Mengontrol akses dengan grup keamanan di Panduan Pengguna Amazon RDS.

Jika Anda menggunakan firewall, batasi akses jaringan ke database dengan mengkonfigurasi ulang Network Access Control Lists (NACLS). Untuk informasi selengkapnya, lihat Firewall AWS Network Firewall di Panduan AWS Network Firewall Pengembang.

Memperbaiki fungsi Lambda yang berpotensi dikompromikan

Saat GuardDuty menghasilkanJenis temuan Perlindungan Lambda, fungsi Lambda Anda dapat dikompromikan. Jika aktivitas yang GuardDuty menyebabkan menghasilkan temuan ini diharapkan, Anda dapat mempertimbangkan untuk menggunakannyaAturan penekanan. Kami merekomendasikan untuk menyelesaikan langkah-langkah berikut untuk memulihkan fungsi Lambda yang dikompromikan:

Untuk memulihkan temuan Perlindungan Lambda

1. Identifikasi versi fungsi Lambda yang berpotensi dikompromikan.

   GuardDuty Temuan untuk Perlindungan Lambda menyediakan nama, Nama Sumber Daya Amazon (ARN), versi fungsi, dan ID revisi yang terkait dengan fungsi Lambda yang tercantum dalam detail temuan.
2. Identifikasi sumber aktivitas yang berpotensi mencurigakan.

   a. Tinjau kode yang terkait dengan versi fungsi Lambda yang terlibat dalam temuan.
   b. Tinjau pustaka dan lapisan yang diimpor dari versi fungsi Lambda yang terlibat dalam temuan.
   c. Jika Anda telah mengaktifkan AWS Lambda fungsi Pemindaian dengan Amazon Inspector, tinjau temuan Amazon Inspector yang terkait dengan fungsi Lambda yang terlibat dalam temuan tersebut.
   d. Tinjau AWS CloudTrail log untuk mengidentifikasi prinsipal yang menyebabkan pembaruan fungsi dan memastikan bahwa aktivitas tersebut diotorisasi atau diharapkan.
3. Memperbaiki fungsi Lambda yang berpotensi terganggu.

   a. Nonaktifkan pemicu eksekusi fungsi Lambda yang terlibat dalam temuan. Untuk informasi selengkapnya, lihat DeleteFunctionEventInvokeConfig.
   b. Tinjau kode Lambda dan perbarui impor pustaka dan lapisan fungsi Lambda untuk menghapus pustaka dan lapisan yang berpotensi mencurigakan.
   c. Mengurangi temuan Amazon Inspector terkait dengan fungsi Lambda yang terlibat dalam temuan tersebut.

Memantau GuardDuty Penggunaan dan Memperkirakan Biaya

GuardDuty menyediakan metrik penggunaan yang melacak pemrosesan sumber data rencana perlindungan logs/events dan vCPU yang dipantau GuardDuty Runtime dari waktu ke waktu.

Di halaman ini:

- Metrik CloudWatch Penggunaan Amazon
- Memahami GuardDuty Penggunaan
- Memperkirakan biaya GuardDuty

Metrik CloudWatch Penggunaan Amazon

GuardDuty menerbitkan metrik penggunaan ke Amazon CloudWatch, memungkinkan Anda untuk:

- Lacak penggunaan aktual dari waktu ke waktu
- Buat dasbor dan alarm khusus
- Ekspor data penggunaan untuk estimasi biaya di Kalkulator AWS Harga

GuardDuty metrik penggunaan dipublikasikan berdasarkan konfigurasi akun Anda:

- Semua akun (mandiri, administrator yang didelegasikan, dan akun anggota) menerima metrik penggunaan akun individual di Amazon CloudWatch
- Akun administrator yang didelegasikan juga menerima metrik penggunaan gabungan untuk seluruh organisasi

GuardDuty metrik penggunaan dipublikasikan di Amazon CloudWatch dalam waktu 24 jam.

Rincian Metrik

GuardDuty menerbitkan metrik penggunaan berikut `Hourly` ke Amazon CloudWatch di bawah `AWS/GuardDuty` namespace:

Rencana Perlindungan	Sumber Data	Nama Metrik	Satuan	Deskripsi
Deteksi Ancaman Dasar	CloudTrailEvents	AnalyzedCount	Hitungan	Jumlah peristiwa CloudTrail manajemen yang dianalisis
Deteksi Ancaman Dasar	VPCFlowLogDNSLogEvents	AnalyzedBytes	Byte	Volume log aliran VPC dan log DNS dianalisis
Perlindungan EKS	KubernetesAuditLogs	AnalyzedCount	Hitungan	Jumlah peristiwa log audit Amazon EKS yang dianalisis
Perlindungan S3	S3DataEvents	AnalyzedCount	Hitungan	Jumlah peristiwa data S3 yang dianalisis
Pemantauan Runtime	RuntimeMonitoringEC2	MonitoredVcpuHours	Hitung (vCPU-Hours)	Jam EC2 vCPU dipantau oleh Pemantauan Runtime
Pemantauan Runtime	RuntimeMonitoringEX	MonitoredVcpuHours	Hitung (vCPU-Hours)	Jam Amazon EKS vCPU dipantau oleh Pemantauan Runtime
Pemantauan Runtime	RuntimeMonitoringFargate	MonitoredVcpuHours	Hitung (vCPU-Hours)	Jam vCPU Fargate dipantau oleh Pemantauan Runtime

Perlindungan Malware untuk EC2	OnDemandEBSSnapshot	ScannedBytes	Byte	Volume data snapshot EBS sesuai permintaan yang dipindai
Perlindungan Malware untuk EC2	OnDemandEBSVolume	ScannedBytes	Byte	Volume data volume EBS sesuai permintaan yang dipindai
Perlindungan Malware untuk EC2	MalwareProtectionEBS	ScannedBytes	Byte	Volume data EBS yang dipindai oleh Malware Protection
Perlindungan RDS	RDS	MonitoredAcuHours	Hitung (ACU-Hours)	Unit Kapasitas Aurora Amazon RDS dipantau
Perlindungan RDS	RDSTanpa batas	MonitoredAcuHours	Hitung (ACU-Hours)	Amazon RDS Aurora Jam ACU tanpa batas dipantau
Perlindungan RDS	AuroraScaleout	MonitoredAcuHours	Hitung (ACU-Hours)	Jam ACU Aurora Scaleout dipantau
Perlindungan RDS	RDS	MonitoredVcpuHours	Hitung (vCPU-Hours)	Jam Amazon RDS vCPU dipantau
Perlindungan Lambda	LambdaNetworkLogs	AnalyzedBytes	Byte	Volume log jaringan Lambda dianalisis

Perlindungan AI	AIDataEvents	AnalyzedBytes	Byte	Volume peristiwa data AI yang dianalisis

Dimensi Metrik

- Semua akun (mandiri, administrator yang didelegasikan, dan akun anggota): Metrik mencakup `DataSource` dimensi `AccountId` dan.
- Akun administrator yang didelegasikan: Metrik juga menyer `DataSource` takan dimensi agregat di semua akun anggota di organisasi.

Perlindungan Malware untuk S3

GuardDuty `Malware Protection for S3`rencana perlindungan menerbitkan metrik penggunaan berikut ke Amazon CloudWatch di bawah `AWS/GuardDuty/MalwareProtection` namespace:

Nama Metrik	Satuan	Deskripsi
CompletedScanCount	Hitungan	Jumlah pemindaian malware objek S3 yang diselesaikan dalam jangka waktu tertentu.
FailedScanCount	Hitungan	Jumlah pemindaian malware objek S3 yang gagal dalam jangka waktu tertentu.
SkippedScanCount	Hitungan	Jumlah pemindaian malware objek S3 yang dilewati dalam jangka waktu tertentu.
InfectedScanCount	Hitungan	Jumlah pemindaian malware objek S3 yang mendeteksi objek yang berpotensi berbahaya dalam jangka waktu tertentu.

CompletedScanBytes	Hitungan	Jumlah byte objek S3 yang dipindai dalam kerangka waktu tertentu.

Dimensi Metrik

- Semua metrik termasuk `Malware Protection Plan Id, Resource Name` dimensi
- SkippedScanCount metrik termasuk `Skipped Reason` sebagai dimensi tambahan

Memahami GuardDuty Penggunaan

GuardDuty Pemrosesan Acara

Saat diaktifkan, GuardDuty secara otomatis mengkonsumsi peristiwa dan log langsung dari sumber log yang Anda pilih Wilayah AWS. GuardDuty mencerna peristiwa dari sumber data independen yang terpisah untuk memberikan nilai keamanan yang komprehensif.

> **Important**
>
> Konfigurasi log layanan individual atau aturan pemfilteran Anda (untuk Log Aliran VPC, Log DNS, CloudTrail Acara, Peristiwa Data S3, Log Audit Kubernetes, dan Log Jaringan Lambda) tidak memengaruhi proses oleh. logs/events GuardDuty

GuardDuty Biaya pemrosesan Log Aliran VPC untuk instans yang dipantau oleh GuardDuty Runtime Monitoring

Untuk instans yang dipantau oleh GuardDuty Runtime Monitoring (melalui agen Runtime EC2 atau agen Runtime Amazon EKS), tidak GuardDuty akan dikenakan biaya untuk pemrosesan Log Aliran VPC selama agen secara aktif mengirimkan data peristiwa runtime. Jika agen berhenti mentransmisikan data peristiwa, kembali GuardDuty ke pengisian melalui Log Aliran VPC.

Mengaktifkan Runtime Monitoring mengurangi penggunaan Log Aliran VPC di metrik CloudWatch penggunaan GuardDuty Amazon. Menonaktifkan Runtime Monitoring mengembalikan penggunaan Log Aliran VPC.

Memperkirakan biaya GuardDuty

GuardDuty menawarkan uji coba gratis 30 hari per AWS akun untuk sebagian besar paket perlindungan. Selama masa percobaan ini, Anda dapat:

- Pantau penggunaan aktual Anda melalui metrik GuardDuty Penggunaan
- Perkirakan biaya bulanan Anda menggunakan Kalkulator AWS Harga berdasarkan pola penggunaan yang Anda amati

Paket perlindungan berikut mencakup uji coba gratis 30 hari:

- Deteksi Ancaman Dasar
- Perlindungan S3
- Perlindungan EKS
- Pemantauan Runtime
- Perlindungan RDS
- Perlindungan Lambda
- Perlindungan AI
- Perlindungan Malware untuk EC2 (hanya untuk GuardDuty-initiated pemindaian saat diaktifkan dengan Deteksi Ancaman Dasar)

Penggunaan AWS Kalkulator Harga

Anda dapat menggunakan Kalkulator AWS Harga untuk memperkirakan GuardDuty biaya bulanan berdasarkan pola penggunaan yang Anda amati. Untuk membuat perkiraan untuk GuardDuty:

1. Buka Kalkulator AWS Harga.
2. Pilih Buat perkiraan.
3. Pada halaman Tambah layanan, cari Amazon GuardDuty dan pilih Konfigurasi.
4. Pilih Wilayah AWS tempat yang GuardDuty diaktifkan.
5. Di bagian Pengaturan layanan, masukkan perkiraan penggunaan Anda untuk setiap paket perlindungan berdasarkan metrik penggunaan yang diamati di Amazon CloudWatch atau GuardDuty konsol.
6. Pilih Tambahkan ke perkiraan saya untuk melihat biaya bulanan yang diproyeksikan.

> **Note**
>
> Beberapa metrik GuardDuty penggunaan dilaporkan dalam byte. Saat memasukkan nilai di Kalkulator AWS Harga, Anda mungkin perlu mengonversi byte ke unit yang sesuai (MB, GB, atau TB). Gunakan konversi berikut:
>
> - 1 MB = 1.048.576 byte
> - 1 GB = 1.073.741.824 byte
> - 1 TB = 1.099.511.627.776 byte

Pelanggan Hub Keamanan

Security Hub menawarkan model harga yang disederhanakan untuk Det GuardDuty eksi Ancaman dengan paket Ancaman Analytics add-on, mengkonsolidasikan pengukuran beberapa. GuardDuty DataSources Saat menggunakan paket Analisis Ancaman Hub Keamanan (Hub Keamanan dengan GuardDuty):

- Beberapa GuardDuty DataSources dikonsolidasikan
- Khususnya, untuk kesederhanaan, peristiwa Log Audit Amazon EKS dan peristiwa Data S3 dikonversi ke GB menggunakan tingkat konversi tetap

Untuk membuat perkiraan biaya Hub Keamanan, silakan merujuk ke Dokumentasi Hub AWS Keamanan.

GuardDutyCatatan: status uji coba gratis 30 hari tidak tergantung pada integrasi Hub Keamanan. Mengaktifkan atau menonaktifkan Hub Keamanan:

- Tidak memberikan uji coba gratis baru jika Anda GuardDuty sudah menggunakan periode uji coba
- Tidak mengganggu atau memulai ulang uji coba gratis yang sedang berlangsung
- Tidak memperpanjang masa percobaan yang ada

Nama fitur untuk paket perlindungan di GuardDuty API

Saat Anda mengaktifkan Amazon GuardDuty untuk pertama kalinya, Amazon mulai diproses Sumber data dasar di AWS lingkungan Anda. GuardDuty menggunakan sumber data ini untuk memproses aliran peristiwa independen seperti log aliran VPC, log DNS, dan AWS CloudTrail peristiwa manajemen. Kemudian menganalisis peristiwa ini untuk mengidentifikasi potensi ancaman keamanan dan menghasilkan temuan di akun Anda.

Ketika satu atau lebih rencana perlindungan diaktifkan, maka GuardDuty gunakan data tambahan dari AWS layanan lain di AWS lingkungan Anda untuk memantau dan menganalisis potensi ancaman keamanan. Sumber data tambahan ini disebut fitur.

Ubah dari sumber data ke fitur

Saat Anda menambahkan GuardDuty perlindungan tambahan, seperti Perlindungan S3, Pemantauan Runtime, Perlindungan Lambda, dan lainnya, Anda dapat mengonfigurasi GuardDuty fitur yang sesuai dengan paket perlindungan. Secara historis, GuardDuty perlindungan dipanggil `dataSources` di API. Namun, setelah Maret 2023, rencana GuardDuty perlindungan baru sekarang dikonfigurasi sebagai `features` dan tidak`dataSources`. GuardDuty masih mendukung konfigurasi rencana perlindungan yang diluncurkan sebelum Maret 2023, seperti `dataSources` melalui API, tetapi rencana perlindungan baru hanya tersedia sebagai. `features` Untuk informasi tentang rencana perlindungan yang terkena dampak, lihatGuardDuty Perubahan API.

Jika Anda mengelola paket GuardDuty konfigurasi dan perlindungan melalui konsol, Anda tidak terpengaruh secara langsung oleh perubahan ini dan tidak perlu mengambil tindakan apa pun. Perubahan ini memengaruhi perilaku API yang dipanggil untuk mengaktifkan GuardDuty atau melindungi rencana di dalamnya GuardDuty. Jika Anda menggunakan API atau AWS CLI untuk mengaktifkan atau mengedit konfigurasi paket perlindungan, Anda harus menggunakan nama fitur terkait. Untuk informasi selengkapnya, lihat Pemetaan ke `dataSources` `features`.

GuardDuty Perubahan API pada Maret 2023

GuardDuty API mengonfigurasi fitur perlindungan yang tidak termasuk dalam daftarGuardDuty sumber data dasar. Objek fitur berisi detail fitur, seperti nama fitur dan status, dan mungkin berisi konfigurasi tambahan untuk beberapa paket perlindungan. Migrasi ini memengaruhi API berikut di Referensi Amazon GuardDuty API:

- CreateDetector
- GetDetector
- UpdateDetector
- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

Fitur dibandingkan dengan sumber data

Secara historis, semua GuardDuty fitur dilewatkan melalui `dataSources` objek di API. Mulai Maret 2023, GuardDuty lebih memilih `features` objek daripada `dataSources` objek di API. Semua sumber data sebelumnya memiliki fitur yang sesuai, tetapi fitur yang lebih baru mungkin tidak memiliki sumber data yang sesuai.

Daftar berikut menunjukkan perbandingan antara `dataSources` dan `features` objek saat melewati API:

- `dataSources`Objek berisi objek untuk setiap jenis perlindungan dan statusnya. `features`Objek adalah daftar fitur yang tersedia yang sesuai dengan setiap jenis perlindungan di dalamnya GuardDuty.

  Mulai Maret 2023, aktivasi fitur akan menjadi satu-satunya cara untuk mengonfigurasi GuardDuty fitur baru di AWS lingkungan Anda.
- `dataSources`Skema dalam permintaan atau respons API sama di setiap Wilayah AWS tempat yang GuardDuty tersedia. Namun, setiap fitur mungkin tidak tersedia di setiap Wilayah. Oleh karena itu, nama fitur yang tersedia mungkin berbeda berdasarkan Wilayah.

Memahami cara kerja API dengan fitur

GuardDuty API akan terus mengembalikan `dataSources` objek sebagaimana berlaku, dan mereka juga akan mengembalikan `features` objek yang berisi informasi yang sama dalam format

yang berbeda. GuardDuty Fitur yang diluncurkan sebelum Maret 2023 akan tersedia melalui `dataSources` objek dan `features` objek. GuardDuty fitur yang diluncurkan sejak Maret 2023 hanya akan tersedia melalui `features` objek. Anda tidak dapat membuat atau memperbarui detektor, atau menjelaskan AWS Organizations penggunaan keduanya `dataSources` dan notasi `features` objek dalam permintaan API yang sama. Untuk mengaktifkan jenis GuardDuty perlindungan, Anda harus memigrasikan sumber data yang ada ke `features` objek dengan menggunakan API yang sama yang sekarang menyertakan `features` objek juga.

> **Note**
>
> GuardDuty tidak akan menambahkan sumber data baru setelah modifikasi ini.

GuardDuty telah menghentikan penggunaan sumber data yang terkait dengan rencana perlindungan. Namun, masih mendukungGuardDuty sumber data dasar. Praktik GuardDuty terbaik merekomendasikan penggunaan fitur untuk mengaktifkan atau mengedit konfigurasi untuk paket perlindungan apa pun di akun Anda.

Memasukkan perubahan fitur dalam API

- Jika Anda mengelola GuardDuty konfigurasi melalui API, SDK, atau CloudFormation template, dan ingin mengaktifkan GuardDuty fitur baru yang potensial, Anda harus memodifikasi kode dan template Anda masing-masing. Untuk informasi selengkapnya, lihat API yang diperbarui di Referensi Amazon GuardDuty API.
- Untuk GuardDuty fitur yang dikonfigurasi sebelum pemutakhiran ini, Anda dapat terus menggunakan API, SDK, atau CloudFormation templat. Namun, kami menyarankan Anda beralih menggunakan `feature` objek.

  Semua sumber data memiliki objek fitur yang setara. Untuk informasi selengkapnya, lihat Pemetaan ke `dataSources` `features`.
- Saat ini, `additionalConfiguration` dalam `features` objek hanya tersedia untuk jenis perlindungan tertentu.
  - Untuk jenis perlindungan seperti itu, jika fitur Anda `AdditionalConfiguration` `status` disetel ke `ENABLED` tetapi konfigurasi fitur Anda tidak `status` disetel ke`ENABLED`, tidak GuardDuty akan mengambil tindakan apa pun dalam kasus ini.
  - API berikut akan terpengaruh oleh ini:
    - UpdateDetector

- UpdateMemberDetectors
- UpdateOrganizationConfiguration

Pemetaan ke `dataSources` `features`

Tabel berikut menunjukkan pemetaan jenis perlindungan,`dataSources`, dan`features`.

GuardDuty jenis perlindungan	Nama sumber data*	Nama fitur
Log Alur VPC	`flowLogs`(baca saja; tidak dapat dimodifikasi)	`FLOW_LOGS` (baca saja; tidak dapat dimodifikasi)
Log kueri DNS Route53 Resolver	`dnsLogs`(baca saja; tidak dapat dimodifikasi)	`DNS_LOGS`(baca saja; tidak dapat dimodifikasi)
CloudTrail acara	`cloudTrail` (baca saja; tidak dapat dimodifikasi)	`CLOUD_TRAIL` (baca saja; tidak dapat dimodifikasi)
S3	`s3Logs`	`S3_DATA_EVENTS`
Perlindungan EKS	`kubernetes.auditlogs`	`EKS_AUDIT_LOGS`
Perlindungan Malware untuk EC2	`malwareProtection.scanEc2InstanceWithFindings.ebsVolumes`	`EBS_MALWARE_PROTECTION`
Acara Login RDS		`RDS_LOGIN_EVENTS`
Pemantauan Runtime EKS	GuardDuty hanya menyediakan dukungan aktivasi fitur untuk jenis perlindungan ini.	`EKS_RUNTIME_MONITORING`
Pemantauan Runtime		`RUNTIME_MONITORING`

GuardDuty jenis perlindungan	Nama sumber data*	Nama fitur

GuardDuty agen keamanan untuk kluster Amazon EKS		`EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`
		
		`RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`

GuardDuty agen keamanan untuk ECS-Fargate cluster Amazon		`RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT`
GuardDuty agen keamanan untuk instans Amazon EC2		`RUNTIME_MONITORING.additionalConfiguration.EC2_AGENT_MANAGEMENT`

GuardDuty jenis perlindungan	Nama sumber data*	Nama fitur
Perlindungan Lambda		`LAMBDA_NETWORK_LOGS`

* GetUsageStatistics menggunakan `dataSource` namanya sendiri. Untuk informasi selengkapnya, lihat Memantau GuardDuty Penggunaan dan Memperkirakan Biaya atau GetUsageStatistics.

Keamanan di Amazon GuardDuty

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model Tanggung Jawab Bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-party Auditor secara teratur menguji dan memverifikasi keefektifan keamanan kami sebagai bagian dari program AWS kepatuhan program AWS . Untuk mempelajari tentang program kepatuhan yang berlaku GuardDuty, lihat AWS layanan dalam cakupan berdasarkan AWS layanan program kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan GuardDuty. Ini menunjukkan kepada Anda cara mengonfigurasi GuardDuty untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan GuardDuty sumber daya Anda.

Konten

- Perlindungan data di Amazon GuardDuty
- Mencatat panggilan GuardDuty API Amazon dengan AWS CloudTrail
- Identity and Access Management untuk Amazon GuardDuty
- Validasi kepatuhan untuk Amazon GuardDuty
- Ketahanan di Amazon GuardDuty
- Keamanan infrastruktur di Amazon GuardDuty
- Amazon GuardDuty dan titik akhir VPC antarmuka ()AWS PrivateLink

Perlindungan data di Amazon GuardDuty

Model tanggung jawab AWS https://aws.amazon.com/compliance/shared-responsibility-model/ berlaku untuk perlindungan data di Amazon GuardDuty. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data Ket . Untuk informasi tentang perlindungan data di Eropa, lihat Pusat Peraturan Umum Perlindungan Data (GDPR).

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredenSIAL dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan CloudTrail jalur untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di Panduan AWS CloudTrail Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan GuardDuty atau Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log

diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi saat diam

Semua data GuardDuty pelanggan dienkripsi saat diam menggunakan solusi AWS enkripsi.

GuardDuty data, seperti temuan, dienkripsi saat diam menggunakan AWS Key Management Service (AWS KMS) dengan kunci AWS yang dimiliki.

Enkripsi saat bergerak

GuardDuty menganalisis data log dari layanan lain. Ini mengenkripsi semua data yang sedang transit dari layanan ini dengan HTTPS dan KMS. Setelah GuardDuty mengekstrak informasi yang dibutuhkan dari log, mereka dibuang. Untuk informasi selengkapnya tentang cara GuardDuty menggunakan informasi dari layanan lain, lihat sumber GuardDuty data.

GuardDuty Data dienkripsi dalam transit antar layanan.

Memilih untuk tidak menggunakan data Anda untuk perbaikan layanan

Anda dapat memilih untuk tidak menggunakan data Anda untuk mengembangkan GuardDuty dan meningkatkan layanan AWS keamanan lainnya dengan menggunakan kebijakan AWS Organizations opt-out. Anda dapat memilih untuk memilih keluar meskipun saat ini GuardDuty tidak mengumpulkan data tersebut. Untuk informasi selengkapnya tentang cara memilih keluar, lihat kebijakan opt-out layanan AI di Panduan AWS Organizations Pengguna.

> **Note**
>
> Agar Anda dapat menggunakan kebijakan opt-out, AWS akun Anda harus dikelola secara terpusat oleh AWS Organizations. Jika Anda belum membuat organisasi untuk AWS akun Anda, lihat Membuat dan mengelola organisasi di Panduan AWS Organizations Pengguna.

Memilih keluar memiliki efek sebagai berikut:

- GuardDuty akan menghapus data yang dikumpulkan dan disimpan untuk tujuan peningkatan layanan sebelum Anda memilih keluar (jika ada).

- Setelah Anda memilih keluar, tidak GuardDuty akan lagi mengumpulkan atau menyimpan data ini untuk tujuan peningkatan layanan.

Topik berikut menjelaskan bagaimana setiap fitur di dalamnya GuardDuty berpotensi menangani data Anda untuk peningkatan layanan.

Daftar Isi

- GuardDuty Pemantauan Runtime
- GuardDuty Perlindungan Malware

GuardDuty Pemantauan Runtime

GuardDuty Runtime Monitoring menyediakan deteksi ancaman runtime untuk cluster Amazon Elastic Kubernetes Service (Amazon EKS), AWS Fargate Amazon Elastic Container Service (Amazon ECS) saja, dan instans Amazon Elastic Compute Cloud (Amazon EC2) di lingkungan Anda. AWS Setelah Anda mengaktifkan Pemantauan Runtime dan menyebarkan agen GuardDuty keamanan untuk sumber daya Anda, GuardDuty mulai memantau dan menganalisis peristiwa runtime yang terkait dengan sumber daya Anda. Jenis peristiwa runtime ini mencakup peristiwa proses, peristiwa kontainer, peristiwa DNS, dan banyak lagi. Untuk informasi selengkapnya, lihat Jenis acara runtime yang dikumpulkan yang menggunakan GuardDuty.

GuardDuty mengumpulkan kedua perintah (seperti`curl`,`systemctl`, dan`cron`) dan argumen terkait (sepertI`start`,`stop`,`disable`) dari beban kerja Anda. Misalnya, ketika seseorang berlari`systemctl stop` *`service-name`*, GuardDuty menangkap perintah `systemctl` dan argumennya`stop` *`service-name`*. Informasi terperinci ini GuardDuty membantu mendeteksi ancaman canggih dengan menganalisis pola perintah dan menghubungkan beberapa peristiwa. Misalnya, GuardDuty dapat mengidentifikasi ketika penyerang mencoba untuk menonaktifkan layanan keamanan atau mengeksekusi file berbahaya yang diketahui. Meskipun GuardDuty secara aktif menggunakan data ini untuk deteksi ancaman, saat ini ia tidak menggunakan perintah dan argumen ini untuk tujuan peningkatan layanan (mungkin melakukannya di masa mendatang). Kepercayaan, privasi, dan keamanan konten Anda adalah prioritas tertinggi kami, dan memastikan bahwa penggunaan kami sesuai dengan komitmen kami kepada Anda. Untuk informasi selengkapnya, lihat FAQ Privasi Data.

GuardDuty Perlindungan Malware

GuardDuty Perlindungan Malware memindai dan mendeteksi malware yang terkandung dalam volume EBS yang melekat pada beban kerja instans dan wadah Amazon EC2 yang berpotensi

terganggu, file yang baru diunggah di bucket Amazon S3 pilihan Anda, dan sumber daya cadangan. Saat ini, GuardDuty tidak mengumpulkan atau menggunakan malware yang terdeteksi untuk peningkatan layanan. Namun, di masa mendatang, ketika GuardDuty Malware Protection mengidentifikasi file volume EBS, file cadangan, atau file S3 sebagai berbahaya atau berbahaya, GuardDuty Malware Protection akan mengumpulkan dan menyimpan file ini untuk mengembangkan dan meningkatkan deteksi malware, dan layanan. GuardDuty File ini juga dapat digunakan untuk mengembangkan dan meningkatkan layanan AWS keamanan lainnya. Kepercayaan, privasi, dan keamanan konten Anda adalah prioritas tertinggi kami, dan memastikan bahwa penggunaan kami sesuai dengan komitmen kami kepada Anda. Untuk informasi selengkapnya, lihat FAQ Privasi Data.

Mencatat panggilan GuardDuty API Amazon dengan AWS CloudTrail

Amazon GuardDuty terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di GuardDuty. CloudTrail menangkap semua panggilan API untuk GuardDuty sebagai peristiwa, termasuk panggilan dari GuardDuty konsol dan dari panggilan kode ke GuardDuty API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon Simple Storage Service (Amazon S3), termasuk acara untuk. GuardDuty Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat GuardDuty, alamat IP tempat permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk informasi selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat Panduan AWS CloudTrail Pengguna.

GuardDuty informasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas acara yang didukung terjadi di GuardDuty, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk GuardDuty, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon

S3. Secara default, ketika Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi lebih lanjut, lihat:

- Ikhtisar untuk membuat jejak
- CloudTraillayanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa wilayah dan Menerima file CloudTrail log dari beberapa akun

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan dibuat dengan pengguna root atau kredenal masuk pengguna IAM
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan
- Apakah permintaan itu dibuat oleh AWS layanan lain

Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.

GuardDuty peristiwa pesawat kontrol di CloudTrail

Secara default, CloudTrail mencatat semua operasi GuardDuty API yang disediakan di Referensi Amazon GuardDuty API sebagai peristiwa dalam CloudTrail file.

GuardDuty peristiwa data di CloudTrail

GuardDuty Pemantauan Runtimemenggunakan agen GuardDuty keamanan yang diterapkan ke kluster Amazon Elastic Kubernetes Service (Amazon EKS), instans Amazon Elastic Compute Cloud (Amazon EC2), dan (Amazon Elastic Container Service (AWS Fargate Amazon ECS) saja) `aws-guardduty-agent` tugas untuk mengumpulkan add-on () yang mengumpulkan beban kerja Anda dan kemudian mengirimkannya Jenis acara runtime yang dikumpulkan ke untuk deteksi dan analisis ancaman. AWS GuardDuty

Pencatatan dan pemantauan peristiwa data

Anda dapat mengonfigurasi AWS CloudTrail log secara opsional untuk melihat peristiwa data untuk agen GuardDuty keamanan Anda.

Untuk membuat dan mengonfigurasi CloudTrail, lihat Peristiwa data di Panduan AWS CloudTrail Pengguna dan ikuti petunjuk untuk Mencatat peristiwa data dengan pemilih peristiwa lanjutan di Konsol Manajemen AWS. Saat mencatat jejak, pastikan untuk membuat perubahan berikut:

- Untuk tipe peristiwa Data, pilih GuardDutydetektor.
- Untuk template pemilih Log, pilih Log semua peristiwa.
- Perluas tampilan JSON untuk konfigurasi. Ini harus mirip dengan JSON berikut:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Setelah Anda mengaktifkan pemilih untuk jejak, navigasikan ke konsol Amazon S3 di. https://console.aws.amazon.com/s3/ Anda dapat mengunduh peristiwa data dari bucket S3 yang dipilih pada saat mengonfigurasi log. CloudTrail

Contoh: entri file GuardDuty log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan peristiwa bidang data.


```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
            "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
            "accountId": "111122223333",
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "111122223333:aws:ec2-instance",
                    "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
                    "accountId": "111122223333",
                    "userName": "aws:ec2-instance"
                },
                "attributes": {
                    "creationDate": "2023-03-05T04:00:21Z",
                    "mfaAuthenticated": "false"
                },
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2023-03-05T06:03:49Z",
        "eventSource": "guardduty.amazonaws.com",
        "eventName": "SendSecurityTelemetry",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "54.240.230.177",
        "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
        "requestParameters": null,
```

```
        "responseElements": null,
        "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
        "readOnly": false,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::GuardDuty::Detector",
            "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
        }
    }
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `CreateIPThreatIntelSet` tindakan (peristiwa bidang kontrol).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-14T22:54:20Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
```

```
            }
        }
    },
    "eventTime": "2018-06-14T22:57:56Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
        "name": "Example",
        "format": "TXT",
        "activate": false,
        "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
        "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```


Dari informasi acara ini, Anda dapat menentukan bahwa permintaan dibuat untuk membuat daftar ancaman `Example` di GuardDuty. Anda juga dapat melihat bahwa permintaan tersebut dibuat oleh pengguna bernama Alice pada 14 Juni 2018.

Identity and Access Management untuk Amazon GuardDuty

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. GuardDuty IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens

- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Amazon GuardDuty bekerja dengan IAM
- Identity-based contoh kebijakan untuk Amazon GuardDuty
- Menggunakan peran terkait layanan untuk Amazon GuardDuty
- AWS kebijakan terkelola untuk Amazon GuardDuty
- Memecahkan masalah GuardDuty identitas dan akses Amazon

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat Memecahkan masalah GuardDuty identitas dan akses Amazon)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Bagaimana Amazon GuardDuty bekerja dengan IAM)
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat Identity-based contoh kebijakan untuk Amazon GuardDuty)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensional dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), otentikasi masuk tunggal, atau kredensional. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensi dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCP) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Amazon GuardDuty bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses GuardDuty, pelajari fitur IAM yang tersedia untuk digunakan. GuardDuty

Fitur IAM yang dapat Anda gunakan dengan Amazon GuardDuty

Fitur IAM	GuardDuty dukungan
Identity-based kebijakan	Ya

Fitur IAM	GuardDuty dukungan
Resource-based kebijakan	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Ya
Service-linked peran	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara GuardDuty dan AWS layanan lain bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Identity-based kebijakan untuk GuardDuty

Mendukung kebijakan berbasis identitas: Ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Identity-based contoh kebijakan untuk GuardDuty

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat. Identity-based contoh kebijakan untuk Amazon GuardDuty

Resource-based kebijakan dalam GuardDuty

Mendukung kebijakan berbasis sumber daya: Tidak

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk GuardDuty

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar GuardDuty tindakan, lihat Tindakan yang ditentukan oleh Amazon GuardDuty di Referensi Otorisasi Layanan.

Tindakan kebijakan GuardDuty menggunakan awalan berikut sebelum tindakan:

```
guardduty
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat. Identity-based contoh kebijakan untuk Amazon GuardDuty

Sumber daya kebijakan untuk GuardDuty

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis GuardDuty sumber daya dan ARNnya, lihat Sumber daya yang ditentukan oleh Amazon GuardDuty di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh Amazon. GuardDuty

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat. Identity-based contoh kebijakan untuk Amazon GuardDuty

Kunci kondisi kebijakan untuk GuardDuty

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci GuardDuty kondisi, lihat Kunci kondisi untuk Amazon GuardDuty di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon GuardDuty.

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat. Identity-based contoh kebijakan untuk Amazon GuardDuty

Daftar kontrol akses (ACL) di GuardDuty

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Attribute-based kontrol akses (ABAC) dengan GuardDuty

Mendukung ABAC (tag dalam kebijakan): Sebagian

Attribute-based Access Control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut yang disebut tag. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensi sementara dengan GuardDuty

Mendukung kredensial sementara: Ya

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Cross-service izin utama untuk GuardDuty

Mendukung sesi akses terusan (FAS): Ya

Sesi akses teruskan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

Peran layanan untuk GuardDuty

Mendukung peran layanan: Ya

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak GuardDuty fungsionalitas. Edit peran layanan hanya jika GuardDuty memberikan panduan untuk melakukannya.

Service-linked peran untuk GuardDuty

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran GuardDuty terkait layanan, lihat. Menggunakan peran terkait layanan untuk Amazon GuardDuty

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Temukan layanan dalam tabel yang `Yes` menyertakan kolom Service-linked peran. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Identity-based contoh kebijakan untuk Amazon GuardDuty

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau mengubah sumber daya GuardDuty. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh GuardDuty, termasuk format ARN untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk Amazon GuardDuty di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan GuardDuty konsol
- Izin diperlukan untuk mengaktifkan GuardDuty
- Mengizinkan pengguna melihat izin mereka sendiri
- Kebijakan IAM khusus untuk memberikan akses hanya-baca ke GuardDuty
- Tolak Akses ke GuardDuty Temuan
- Menggunakan kebijakan IAM khusus untuk membatasi akses ke sumber daya GuardDuty

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus GuardDuty sumber daya di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan.

Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan GuardDuty konsol

Untuk mengakses GuardDuty konsol Amazon, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang GuardDuty sumber daya di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan GuardDuty konsol, lampirkan juga kebijakan GuardDuty `ConsoleAccess` atau `ReadOnly` AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Izin diperlukan untuk mengaktifkan GuardDuty

Untuk memberikan izin yang harus dimiliki oleh berbagai identitas IAM (pengguna, grup, dan peran), lampirkan AWS kebijakan yang dikelola: AmazonGuardDutyFullAccess_v2 (direkomendasikan) kebijakan yang diperlukan untuk mengaktifkan. GuardDuty

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. 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": "*"
        }
    ]
}
```

Kebijakan IAM khusus untuk memberikan akses hanya-baca ke GuardDuty

Untuk memberikan akses hanya-baca ke GuardDuty Anda dapat menggunakan kebijakan `AmazonGuardDutyReadOnlyAccess` terkelola.

Untuk membuat kebijakan kustom yang memberikan akses hanya baca peran IAM, pengguna, atau grup GuardDuty, Anda dapat menggunakan pernyataan berikut:

JSON

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

```
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
                "guardduty:ListDetectors",
                "guardduty:GetDetector",
                "guardduty:ListFindings",
                "guardduty:GetFindings",
                "guardduty:ListIPSets",
                "guardduty:GetIPSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:GetThreatIntelSet",
                "guardduty:GetMasterAccount",
                "guardduty:GetInvitationsCount",
                "guardduty:GetFindingsStatistics",
                "guardduty:DescribeMalwareScans",
                "guardduty:UpdateMalwareScanSettings",
                "guardduty:GetMalwareScanSettings"
            ],
            "Resource": "*"
        }
    ]
}
```

Tolak Akses ke GuardDuty Temuan

Anda dapat menggunakan kebijakan berikut untuk menolak peran IAM, pengguna, atau akses grup ke GuardDuty temuan. Pengguna tidak dapat melihat temuan atau detail tentang temuan, tetapi mereka dapat mengakses semua GuardDuty operasi lainnya:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateDetector",
```

```
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "guardduty:CreateIPSet",
                "guardduty:DeleteIPSet",
                "guardduty:UpdateIPSet",
                "guardduty:GetIPSet",
                "guardduty:ListIPSets",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:UpdateThreatIntelSet",
                "guardduty:GetThreatIntelSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:ArchiveFindings",
                "guardduty:UnarchiveFindings",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateMembers",
                "guardduty:InviteMembers",
                "guardduty:GetMembers",
                "guardduty:DeleteMembers",
                "guardduty:DisassociateMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:ListMembers",
                "guardduty:GetMasterAccount",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:AcceptAdministratorInvitation",
                "guardduty:ListInvitations",
                "guardduty:GetInvitationsCount",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteInvitations"
            ],
            "Resource": "*"
        },
         {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
```

```
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Menggunakan kebijakan IAM khusus untuk membatasi akses ke sumber daya GuardDuty

Untuk menentukan akses pengguna GuardDuty berdasarkan ID detektor, Anda dapat menggunakan semua tindakan GuardDuty API dalam kebijakan IAM kustom, kecuali operasi berikut:

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Gunakan operasi berikut dalam kebijakan IAM untuk menentukan akses pengguna GuardDuty berdasarkan ID dan ThreatIntelSet ID IPSet:

- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`

- `guardduty:UpdateThreatIntelSet`

Contoh berikut ini menunjukkan cara membuat kebijakan menggunakan beberapa operasi sebelumnya:

- Kebijakan ini memungkinkan pengguna untuk menjalankan operasi `guardduty:UpdateDetector`, menggunakan ID detektor 1234567 di Wilayah us-east-1:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateDetector"
            ],
            "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567"
        }
    ]
}
```

- Kebijakan ini memungkinkan pengguna untuk menjalankan operasi `guardduty:UpdateIPSet`, menggunakan ID detektor 1234567 dan ID IPSet 000000 di Wilayah us-east-1:

> **Note**
>
> Pastikan bahwa pengguna memiliki izin yang diperlukan untuk mengakses daftar IP tepercaya dan daftar ancaman di GuardDuty. Untuk informasi selengkapnya, lihat Menyiapkan prasyarat untuk daftar entitas dan daftar alamat IP.

  JSON

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

```
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet"
            ],
            "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567/ipset/000000"
        }
    ]
}
```

- Kebijakan ini memungkinkan pengguna untuk menjalankan operasi `guardduty:UpdateIPSet`, menggunakan ID detektor dan ID IPSet 000000 di Wilayah us-east-1:

> **Note**
>
> Pastikan bahwa pengguna memiliki izin yang diperlukan untuk mengakses daftar IP tepercaya dan daftar ancaman di GuardDuty. Untuk informasi selengkapnya, lihat Menyiapkan prasyarat untuk daftar entitas dan daftar alamat IP.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet"
            ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- Kebijakan ini memungkinkan pengguna untuk menjalankan `guardduty:UpdateIPSet` operasi, menggunakan ID detektor dan ID IPSet apa pun di Wilayah us-east-1:

> **Note**
>
> Pastikan bahwa pengguna memiliki izin yang diperlukan untuk mengakses daftar IP tepercaya dan daftar ancaman di GuardDuty. Untuk informasi selengkapnya, lihat Menyiapkan prasyarat untuk daftar entitas dan daftar alamat IP.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet"
            ],
            "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567/ipset/*"
        }
    ]
}
```

ARN sumber daya IAM untuk tindakan cocok GuardDuty dengan jalur sumber daya API tindakan tersebut. Sebagian besar tindakan memetakan ke detektor atau sub-sumber daya. Misalnya, `guardduty:GetDetector` penggunaan`detector/detectorId`, dan `guardduty:GetFilter` penggunaan`detector/detectorId/filter/filterName`.

Sebagian besar temuan dan tindakan anggota menambahkan nama operasi sebagai akhiran di jalur sumber daya. Operasi daftar adalah pengecualian: `guardduty:ListFindings` dan `guardduty:ListMembers` gunakan basis `findings` dan `member` jalur tanpa akhiran. Sertakan jalur lengkap saat Anda mencakup kebijakan untuk tindakan ini:

- `guardduty:GetFindings`menggunakan `detector/detectorId/findings/get`
- `guardduty:GetFindingsStatistics`menggunakan `detector/detectorId/findings/statistics`
- `guardduty:ArchiveFindings`menggunakan `detector/detectorId/findings/archive`

- `guardduty:GetMembers`menggunakan `detector/detectorId/member/get`
- `guardduty:ListFindings`menggunakan `detector/detectorId/findings` (tidak ada akhiran)
- `guardduty:ListMembers`menggunakan `detector/detectorId/member` (tidak ada akhiran)

Kebijakan berikut memberikan detektor tertentu `guardduty:GetFindings` di Wilayah us-east-1, menggunakan jalur sumber daya lengkap:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "guardduty:GetFindings",
    "Resource": "arn:aws:guardduty:us-
east-1:111122223333:detector/a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6/findings/get"
  }]
}
```

Menggunakan peran terkait layanan untuk Amazon GuardDuty

Amazon GuardDuty menggunakan peran AWS Identity and Access Management terkait layanan (IAM). Peran terkait layanan (SLR) adalah jenis peran IAM unik yang ditautkan langsung ke. GuardDuty Service-linked peran telah ditentukan sebelumnya oleh GuardDuty dan menyertakan semua izin yang GuardDuty diperlukan untuk memanggil AWS layanan lain atas nama Anda.

Dengan peran terkait layanan, Anda dapat mengatur GuardDuty tanpa menambahkan izin yang diperlukan secara manual. GuardDuty mendefinisikan izin dari peran yang ditautkan layanan, dan kecuali izin ditentukan sebaliknya, hanya GuardDuty dapat mengambil peran tersebut. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

GuardDuty mendukung penggunaan peran terkait layanan di semua Wilayah yang GuardDuty tersedia. Untuk informasi selengkapnya, lihat Wilayah dan titik akhir.

Anda dapat menghapus peran yang GuardDuty ditautkan layanan hanya setelah pertama kali menonaktifkan GuardDuty di semua Wilayah yang diaktifkan. Ini melindungi GuardDuty sumber daya Anda karena Anda tidak dapat menghapus izin untuk mengaksesnya secara tidak sengaja.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM dan cari layanan yang memiliki Ya di kolom Peran. Service-Linked Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Service-linked izin peran untuk GuardDuty

GuardDuty menggunakan peran terkait layanan (SLR) bernama. `AWSServiceRoleForAmazonGuardDuty` SLR memungkinkan GuardDuty untuk melakukan tugas-tugas berikut. Ini juga memungkinkan GuardDuty untuk memasukkan metadata yang diambil milik instance EC2 dalam temuan yang GuardDuty mungkin dihasilkan tentang potensi ancaman. Peran terkait layanan `AWSServiceRoleForAmazonGuardDuty` memercayai layanan `guardduty.amazonaws.com` untuk menjalankan peran.

Kebijakan izin membantu GuardDuty melakukan tugas-tugas berikut:

- Gunakan tindakan Amazon EC2 untuk mengelola dan mengambil informasi tentang instans EC2, gambar, dan komponen jaringan seperti VPC, subnet, dan gateway transit.
- Gunakan AWS Systems Manager tindakan untuk mengelola asosiasi SSM pada instans Amazon EC2 saat Anda mengaktifkan Pemantauan GuardDuty Runtime dengan agen otomatis untuk Amazon EC2. Saat konfigurasi agen GuardDuty otomatis dinonaktifkan, GuardDuty pertimbangkan hanya instans EC2 yang memiliki tag inklusi (`GuardDutyManaged:true`).
- Gunakan AWS Organizations tindakan untuk menjelaskan akun terkait dan ID organisasi.
- Gunakan tindakan Amazon S3 untuk mengambil informasi tentang bucket dan objek S3.
- Gunakan AWS Lambda tindakan untuk mengambil informasi tentang fungsi dan tag Lambda Anda.
- Gunakan tindakan Amazon EKS untuk mengelola dan mengambil informasi tentang cluster EKS dan mengelola add-on Amazon EKS di cluster EKS. Tindakan EKS juga mengambil informasi tentang tag yang terkait dengan GuardDuty.
- Gunakan IAM untuk membuat Per Service-linked izin peran untuk Perlindungan Malware untuk EC2 lindungan Malware setelah EC2 diaktifkan.
- Gunakan tindakan Amazon ECS untuk mengelola dan mengambil informasi tentang cluster Amazon ECS, mengambil informasi tentang tugas dan definisi tugas, dan mengelola pengaturan akun Amazon ECS dengan. `guarddutyActivate` Tindakan yang berkaitan dengan Amazon ECS juga mengambil informasi tentang tag yang terkait dengannya GuardDuty.
- Gunakan tindakan Amazon VPC Lattice untuk mengaktifkan konektivitas untuk agen Runtime Monitoring.

Peran dikonfigurasi dengan kebijakan terkel AWS ola berikut, bernama`AmazonGuardDutyServiceRolePolicy`.

Untuk meninjau izin kebijakan ini, lihat AmazonGuardDutyServiceRolePolicy di Panduan Referensi AWS Kebijakan Terkelola.

Berikut ini adalah kebijakan kepercayaan yang dilampirkan ke peran yang terhubung dengan layanan `AWSServiceRoleForAmazonGuardDuty`:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Untuk detail tentang pembaruan `AmazonGuardDutyServiceRolePolicy` kebijakan, lihatGuardDuty update ke AWS kebijakan terkelola. Untuk peringatan otomatis tentang perubahan kebijakan ini, berlangganan umpan RSS di Riwayat dokumen halaman.

Membuat peran terkait layanan untuk GuardDuty

Per `AWSServiceRoleForAmazonGuardDuty` an tertaut layanan dibuat secara otomatis saat Anda mengaktifkan GuardDuty untuk pertama kalinya atau mengaktifkan GuardDuty di Wilayah yang didukung di mana sebelumnya Anda tidak mengaktifkannya. Anda juga dapat membuat peran terkait layanan secara manual menggunakan konsol IAM, API AWS CLI, atau IAM.

> **Important**
>
> Peran terkait layanan yang dibuat untuk akun administrator yang GuardDuty didelegasikan tidak berlaku untuk akun anggota GuardDuty .

Anda harus mengonfigurasi izin untuk mengizinkan prinsipal IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Agar peran `AWSServiceRoleForAmazonGuardDuty` terkait layanan berhasil dibuat, prinsipal IAM yang Anda gunakan harus memiliki GuardDuty izin yang diperlukan. Untuk memberikan izin yang diperlukan, lampirkan kebijakan berikut ke pengguna, grup, atau peran ini:

> **Note**
>
> Ganti sampel *`account ID`* dalam contoh berikut dengan Akun AWS ID Anda yang sebenarnya.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
```

```
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Untuk informasi selengkapnya tentang membuat peran secara manual, lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM.

Mengedit peran terkait layanan untuk GuardDuty

GuardDuty tidak mengizinkan Anda mengedit peran yang dit `AWSServiceRoleForAmazonGuardDuty` autkan layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran yang ditautkan layanan untuk GuardDuty

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dikelola secara aktif.

> **Important**
>
> Jika Anda telah mengaktifkan Perlindungan Malware untuk EC2, menghapus `AWSServiceRoleForAmazonGuardDuty` tidak akan dihapus secara otomatis. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Jika Anda ingin menghapus`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, lihat Menghapus peran terkait layanan untuk Perlindungan Malware untuk EC2.

Anda harus menonaktifkan terlebih dahulu GuardDuty di semua Wilayah di mana itu diaktifkan untuk menghapus`AWSServiceRoleForAmazonGuardDuty`. Jika GuardDuty layanan tidak dinonaktifkan saat Anda mencoba menghapus peran terkait layanan, penghapusan gagal. Untuk informasi selengkapnya, lihat Menangguhkan atau menonaktifkan GuardDuty.

Saat Anda menonaktifkan GuardDuty, `AWSServiceRoleForAmazonGuardDuty` tidak akan dihapus secara otomatis. Jika Anda mengaktifkan GuardDuty lagi, itu akan mulai menggunakan yang sudah ada`AWSServiceRoleForAmazonGuardDuty`.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau IAM API untuk menghapus peran terkait layanan`AWSServiceRoleForAmazonGuardDuty`. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Didukung Wilayah AWS

Amazon GuardDuty mendukung penggunaan peran `AWSServiceRoleForAmazonGuardDuty` terkait layanan di semua Wilayah AWS tempat yang GuardDuty tersedia. Untuk daftar Wilayah yang saat GuardDuty ini tersedia, lihat GuardDuty titik akhir dan kuota Amazon di Referensi Umum Amazon Web.

Service-linked izin peran untuk Perlindungan Malware untuk EC2

Perlindungan Malware untuk EC2 menggunakan peran terkait layanan (SLR) bernama. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` SLR ini memungkinkan Perlindungan Malware untuk EC2 melakukan pemindaian tanpa agen untuk mendeteksi malware di akun Anda. GuardDuty Ini memungkinkan GuardDuty untuk membuat snapshot volume EBS di akun Anda, dan berbagi snapshot itu dengan akun GuardDuty layanan. Setelah GuardDuty mengevaluasi snapshot, ia menyertakan instance EC2 yang diambil dan metadata beban kerja kontainer dalam Perlindungan Malware untuk temuan EC2. Peran terkait layanan `AWSServiceRoleForAmazonGuardDutyMalwareProtection` memercayai layanan `malware-protection.guardduty.amazonaws.com` untuk menjalankan peran.

Kebijakan izin untuk peran ini membantu Perlindungan Malware untuk EC2 untuk melakukan tugas-tugas berikut:

- Gunakan tindakan Amazon Elastic Compute Cloud (Amazon EC2) untuk mengambil informasi tentang instans, volume, dan snapshot Amazon EC2 Anda. Perlindungan Malware untuk EC2 juga memberikan izin untuk mengakses metadata cluster Amazon EKS dan Amazon ECS.
- Buat snapshot untuk volume EBS yang tidak disetel `GuardDutyExcluded` tag ke. `true` Secara default, snapshot dibuat dengan `GuardDutyScanId` tag. Jangan hapus tag ini, jika tidak Perlindungan Malware untuk EC2 tidak akan memiliki akses ke snapshot.

> **Important**
>
> Saat Anda menyet `true` el `GuardDutyExcluded` ke, GuardDuty layanan tidak akan dapat mengakses snapshot ini di masa mendatang. Ini karena pernyataan lain dalam peran terkait layanan ini GuardDuty mencegah melakukan tindakan apa pun pada snapshot yang disetel ke`GuardDutyExcluded`. `true`

- Izinkan berbagi dan menghapus snapshot hanya jika `GuardDutyScanId` tag ada dan `GuardDutyExcluded` tag tidak disetel ke`true`.

> **Note**
>
> Tidak mengizinkan Perlindungan Malware untuk EC2 membuat snapshot menjadi publik.

- Akses kunci yang dikelola pelanggan, kecuali kunci yang memiliki `GuardDutyExcluded` tag diset `true` el ke, `CreateGrant` untuk memanggil untuk membuat dan mengakses volume EBS terenkripsi dari snapshot terenkripsi yang dibagikan dengan akun GuardDuty layanan. Untuk daftar akun GuardDuty layanan untuk setiap Wilayah, lihat[GuardDuty akun layanan oleh Wilayah AWS](#).
- Akses CloudWatch log pelanggan untuk membuat grup log Perlindungan Malware untuk EC2 serta menempatkan log peristiwa pemindaian malware di bawah grup `/aws/guardduty/malware-scan-events` log.
- Izinkan pelanggan untuk memutuskan apakah mereka ingin menyimpan snapshot di mana malware terdeteksi, di akun mereka. Jika pemindaian mendeteksi malware, peran terkait layanan memungkinkan GuardDuty untuk menambahkan dua tag ke snapshot - dan. `GuardDutyFindingDetected` `GuardDutyExcluded`

> **Note**
>
> `GuardDutyFindingDetected`Tag menentukan bahwa snapshot berisi malware.

- Tentukan apakah volume dienkripsi dengan kunci yang dikelola EBS. GuardDuty melakukan `DescribeKey` tindakan untuk menentukan `key Id` EBS-managed kunci di akun Anda.
- Ambil snapshot volume EBS yang dienkripsi menggunakan Kunci yang dikelola AWS, dari Anda Akun AWS dan salin ke. [GuardDuty akun layanan](#) Untuk tujuan ini, kami menggunakan izin `GetSnapshotBlock` dan`ListSnapshotBlocks`. GuardDuty kemudian akan memindai snapshot di akun layanan. Saat ini, dukungan Perlindungan Malware untuk EC2 untuk pemindaian volume

EBS yang dienkripsi Kunci yang dikelola AWS mungkin tidak tersedia di semua. Wilayah AWS Untuk informasi selengkapnya, lihat Region-specific ketersediaan fitur.

- Izinkan Amazon EC2 menelep AWS KMS on atas nama Malware Protection for EC2 untuk melakukan beberapa tindakan kriptografi pada kunci yang dikelola pelanggan. Tindakan seperti `kms:ReEncryptTo` dan `kms:ReEncryptFrom` diperlukan untuk berbagi snapshot yang dienkripsi dengan kunci yang dikelola pelanggan. Hanya kunci yang dapat diakses yang tidak disetel `GuardDutyExcluded` tagnya`true`.

Peran dikonfigurasi dengan kebijakan terkel AWS ola berikut, bernama`AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

Untuk meninjau izin kebijakan ini, lihat AmazonGuardDutyMalwareProtectionServiceRolePolicy di Panduan Referensi AWS Kebijakan Terkelola.

Kebijakan kepercayaan berikut dilampirkan pada peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Membuat peran terkait layanan untuk Perlindungan Malware untuk EC2

Per `AWSServiceRoleForAmazonGuardDutyMalwareProtection` an terkait layanan dibuat secara otomatis saat Anda mengaktifkan Perlindungan Malware untuk EC2 untuk pertama kalinya atau mengaktifkan Perlindungan Malware untuk EC2 di Wilayah yang didukung di mana sebelumnya Anda tidak mengaktifkannya. Anda juga dapat membuat peran tertaut layanan

`AWSServiceRoleForAmazonGuardDutyMalwareProtection` secara manual menggunakan konsol IAM, CLI IAM, atau API IAM.

> **Note**
>
> Secara default, jika Anda baru mengenal Amazon GuardDuty, Perlindungan Malware untuk EC2 secara otomatis diaktifkan.

> **Important**
>
> Peran terkait layanan yang dibuat untuk akun GuardDuty administrator yang didelegasikan tidak berlaku untuk akun anggota GuardDuty .

Anda harus mengonfigurasi izin untuk mengizinkan prinsipal IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Agar peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan berhasil dibuat, identitas IAM yang Anda gunakan harus memiliki GuardDuty izin yang diperlukan. Untuk memberikan izin yang diperlukan, lampirkan kebijakan berikut ke pengguna, grup, atau peran ini:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

Untuk informasi selengkapnya tentang membuat peran secara manual, lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM.

Mengedit peran terkait layanan untuk Perlindungan Malware untuk EC2

Perlindungan Malware untuk EC2 tidak memungkinkan Anda mengedit peran terkait `AWSServiceRoleForAmazonGuardDutyMalwareProtection` layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Perlindungan Malware untuk EC2

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dikelola secara aktif.

> **Important**
>
> Untuk menghapus`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, Anda harus terlebih dahulu menonaktifkan Perlindungan Malware untuk EC2 di semua Wilayah di mana ia diaktifkan.
> Jika Perlindungan Malware untuk EC2 tidak dinonaktifkan saat Anda mencoba menghapus peran terkait layanan, penghapusan akan gagal. Pastikan bahwa Anda terlebih dahulu menonaktifkan Perlindungan Malware untuk EC2 di akun Anda.

Ketika Anda memilih N onaktifkan untuk menghentikan Perlindungan Malware untuk layanan EC2, layanan tersebut `AWSServiceRoleForAmazonGuardDutyMalwareProtection` tidak dihapus secara otomatis. Jika Anda kemudian memilih Aktif kan untuk memulai Perlindungan Malware untuk layanan EC2 lagi, GuardDuty akan mulai menggunakan yang sudah ada`AWSServiceRoleForAmazonGuardDutyMalwareProtection`.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau IAM API untuk menghapus peran terkait layanan. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Didukung Wilayah AWS

Amazon GuardDuty mendukung penggunaan peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan di semua Wilayah AWS tempat Perlindungan Malware untuk EC2 tersedia.

Untuk daftar Wilayah yang saat GuardDuty ini tersedia, lihat GuardDuty titik akhir dan kuota Amazon di Referensi Umum Amazon Web.

AWS kebijakan terkelola untuk Amazon GuardDuty

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan yang dikelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan terkel AWS ola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di Akun AWS Anda. Untuk informasi

selengkapnya tentang AWS kebijakan terkelola, AWS lihat kebijakan ter kelola di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan ter AWS kelola. Layanan terkadang menambahkan izin tambahan ke kebijakan ter AWS kelola untuk mendukung fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan AWS terkelola saat fitur baru diluncurkan atau ketika operasi baru tersedia. Layanan tidak menghapus izin dari kebijakan ter AWS kelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan terkel ReadOnlyAccess AWS ola menyediakan akses baca-saja ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS menambahkan izin baca-saja untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat kebijakan yang dikelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

Elemen kebijakan `Version` menetapkan aturan sintaksis bahasa yang akan digunakan untuk memproses kebijakan. Kebijakan berikut mencakup versi saat ini yang didukung IAM. Untuk informasi selengkapnya, lihat elemen kebijakan JSON IAM: Versi.

AWS kebijakan yang dikelola: AmazonGuardDutyFullAccess_v2 (direkomendasikan)

Anda dapat melampirkan kebijakan AmazonGuardDutyFullAccess_v2 ke identitas IAM Anda. Kebijakan ini akan memungkinkan pengguna akses penuh untuk melakukan semua GuardDuty tindakan dan mengakses sumber daya yang diperlukan. Antara AmazonGuardDutyFullAccess_v2 dan AmazonGuardDutyFullAccess, GuardDuty merekomendasikan melampirkan AmazonGuardDutyFullAccess_v2 karena menawarkan keamanan yang ditingkatkan dan membatasi tindakan administratif untuk prinsipal GuardDuty layanan.

Detail izin

AmazonGuardDutyFullAccess_v2Kebijakan ini mencakup izin berikut:

- `GuardDuty`- Memungkinkan pengguna akses penuh ke semua GuardDuty tindakan.
- `IAM`:
  - Memungkinkan pengguna untuk membuat GuardDuty peran terkait layanan.

  - Memungkinkan melihat dan mengelola peran IAM dan kebijakannya untuk GuardDuty.
  - Memungkinkan pengguna untuk meneruskan peran ke GuardDuty. GuardDuty menggunakan peran ini untuk mengaktifkan Perlindungan Malware untuk S3 dan memindai objek S3 untuk malware. GuardDuty juga menggunakan peran ini untuk memulai pemindaian untuk Perlindungan Malware untuk AWS Cadangan.
  - Izin untuk melakukan `iam:GetRole` tindakan `AWSServiceRoleForAmazonGuardDutyMalwareProtection` menetapkan jika peran terkait layanan (SLR) untuk Perlindungan Malware untuk EC2 ada di akun.
- `Organizations`:
  - Izinkan pengguna membaca (melihat) struktur GuardDuty organisasi dan akun.
  - Memungkinkan pengguna untuk menunjuk administrator yang didelegasikan dan mengelola anggota untuk GuardDuty organisasi.

Untuk meninjau izin kebijakan ini, lihat AmazonGuardDutyFullAccess _v2 di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan yang dikelola: AmazonGuardDutyFullAccess

Anda dapat melampirkan kebijakan `AmazonGuardDutyFullAccess` ke identitas IAM Anda.

> **Important**
>
> Untuk keamanan yang ditingkatkan dan izin terbatas untuk GuardDuty prinsipal layanan, kami sarankan Anda untuk menggunakannyaAWS kebijakan yang dikelola: AmazonGuardDutyFullAccess_v2 (direkomendasikan).

Kebijakan ini memberikan izin administratif yang memungkinkan pengguna akses penuh untuk melakukan semua GuardDuty tindakan dan sumber daya.

Detail izin

Kebijakan ini mencakup izin berikut.

- `GuardDuty`- Memungkinkan pengguna akses penuh ke semua GuardDuty tindakan.

- `IAM`:
  - Memungkinkan pengguna untuk membuat peran GuardDuty terkait layanan.
  - Mengizinkan akun administrator GuardDuty untuk mengaktifkan akun anggota.
  - Memungkinkan pengguna untuk meneruskan peran ke GuardDuty. GuardDuty menggunakan peran ini untuk mengaktifkan Perlindungan Malware untuk S3 dan memindai objek S3 untuk malware. GuardDuty juga menggunakan peran ini untuk memulai pemindaian untuk Perlindungan Malware untuk AWS Cadangan.
- `Organizations`- Memungkinkan pengguna untuk menunjuk administrator yang didelegasikan dan mengelola anggota untuk GuardDuty organisasi.

Izin untuk melakukan `iam:GetRole` tindakan `AWSServiceRoleForAmazonGuardDutyMalwareProtection` menetapkan jika peran terkait layanan (SLR) untuk Perlindungan Malware untuk EC2 ada di akun.

Untuk meninjau izin kebijakan ini, lihat AmazonGuardDutyFullAccess di Panduan Referensi AWS Kebijakan Terkelola.

AWS kebijakan yang dikelola: AmazonGuardDutyReadOnlyAccess

Anda dapat melampirkan kebijakan `AmazonGuardDutyReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin baca-saja yang memungkinkan pengguna melihat GuardDuty temuan dan detail organisasi Anda GuardDuty .

Detail izin

Kebijakan ini mencakup izin berikut.

- `GuardDuty`- Memungkinkan pengguna untuk melihat GuardDuty temuan dan melakukan operasi API yang dimulai dengan`Get`,`List`, atau`Describe`.
- `Organizations`- Memungkinkan pengguna mengambil informasi tentang konfigurasi GuardDuty organisasi Anda, termasuk rincian akun administrator yang didelegasikan.

Untuk meninjau izin kebijakan ini, lihat AmazonGuardDutyReadOnlyAccess di Panduan Referensi AWS Kebijakan Terkelola.

AWS kebijakan yang dikelola: AmazonGuardDutyServiceRolePolicy

Anda tidak dapat melampirkan `AmazonGuardDutyServiceRolePolicy` ke entitas IAM Anda. Kebijakan AWS terkelola ini dilampirkan ke peran terkait layanan yang memungkinkan GuardDuty untuk melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Service-linked izin peran untuk GuardDuty.

GuardDuty update ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola GuardDuty sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman GuardDuty riwayat dokumen.

Ubah	Deskripsi	Tanggal
AmazonGuardDutyServiceRolePolicy — Permbaruan ke kebijakan yang sudah ada	Menambahkan `vpc-lattice:AssociateViaAWSService` izin `vpc-lattice:CreateServiceNetworkVpcAssociation` dan, yang memungkinkan GuardDuty untuk menggunakan tindakan Amazon VPC Lattice untuk mengaktifkan konektivitas untuk agen Runtime Monitoring. Per `GdLatticeCreateManagedSnvaAssociation` nyataan ini memungkinkan GuardDuty untuk membuat asosiasi VPC jaringan layanan untuk sumber daya di akun yang sama. Per `GdLatticeAssociateViaAwsService` nyataan tersebut memungkinkan GuardDuty	September 9, 2026

Ubah	Deskripsi	Tanggal

	untuk menyelesaikan asosiasi melalui Amazon VPC Lattice.
	
	{
	
	"Sid": "GdLatticeCreateManagedSnvaAssociation",
	
	"Effect": "Allow",
	
	"Action": "vpc-lattice:CreateServiceNetworkVpcAssociation",
	
	"Resource": "arn:aws:vpc-lattice:*:*:servicenetworkvpcassociation/*",
	
	"Condition": {
	
	"StringEquals": {
	
	"aws:ResourceAccount": "${aws:PrincipalAccount}"
	
	}
	
	}
	
	},
	
	{
	
	"Sid": "GdLattic	

Ubah	Deskripsi	Tanggal

	<pre>eAssociateViaAwsSe
	rvice",
	
	"Effect":
	"Allow",
	
	"Action": "vpc-
	lattice:AssociateViaAW
	SService",
	
	"Resource": "*"
	
	}</pre>	

AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan `s3:ListBucket` izin untuk mengambil daftar bucket S3, `ecs:DescribeTasks` dan `ecs:DescribeTaskDefinition` izin untuk mengambil informasi tentang tugas Amazon ECS dan definisi tugas.	April 23, 2026

Ubah	Deskripsi	Tanggal
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan `cloudtrail:CreateServiceLinkedChannel` izin untuk mengaktifkan mekanisme tambahan untuk mengkonsumsi AWS CloudTrail acara. `{ "Sid": "CloudTrailCreateServiceLinkedChannelSid", "Effect": "Allow", "Action": [ "cloudtrail:CreateServiceLinkedChannel" ], "Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/guardduty/*", "Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}"`	Maret 25, 2026

Ubah	Deskripsi	Tanggal

	<pre>}
	}
	}</pre>	

`AmazonGuardDutyFullAccess` — Tidak digunakan lagi	Kebijakan ini telah digantikan oleh kebijakan dengan cakupan yang diberi nama. `AmazonGuardDutyFullAccess_v2` Setelah 13 Maret 2026, Anda tidak dapat melampirkan `AmazonGuardDutyFullAccess` kebijakan ke pengguna, grup, atau peran baru. Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola: AmazonGuardDutyFullAccess_v2 (direkomendasikan).	Maret 13, 2026

Ubah	Deskripsi	Tanggal

AmazonGuardDutyFullAccess_v2 – Pembaruan ke kebijakan yang ada	Menambahkan izin yang memungkinkan Anda untuk meneruskan peran IAM GuardDuty saat Anda mengaktifkan Perlindungan Malware untuk AWS Cadangan.
	
	{
	"Sid": "AllowPassRoleToMalwareProtection",
	"Effect": "Allow",
	"Action": [
	"iam:PassRole"
	],
	"Resource": "arn:aws:iam::*:role/*",
	"Condition": {
	"StringEquals": {
	"iam:PassedToService": [
	"malware-protectio
		November 19, 2025

Ubah	Deskripsi	Tanggal
	n-plan.guardduty.amazonaws.com", "malware-protection.guardduty.amazonaws.com"] } } }	

Ubah	Deskripsi	Tanggal

AmazonGuardDutyFullAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin yang memungkinkan Anda untuk meneruskan peran IAM GuardDuty saat Anda mengaktifkan Perlindungan Malware untuk AWS Cadangan.
	
	{
	"Sid": "AllowPassRoleToMalwareProtection",
	"Effect": "Allow",
	"Action": [
	"iam:PassRole"
	],
	"Resource": "arn:aws:iam::*:role/*",
	"Condition": {
	"StringEquals": {
	"iam:PassedToService": [
	"malware-protectio
		November 19, 2025

Ubah	Deskripsi	Tanggal
	n-plan.guardduty.amazonaws.com", "malware-protection.guardduty.amazonaws.com"] } } }	
AmazonGuardDutyFullAccess_v2— Menambahkan kebijakan baru	Menambahkan AmazonGuardDutyFullAccess_v2 kebijakan baru. Ini direkomendasikan karena izinnya meningkatkan keamanan dengan membatasi tindakan administratif untuk GuardDuty prinsipal layanan berdasarkan peran dan kebijakan IAM, serta integrasi. AWS Organizations	04 Juni 2025
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan `ec2:DescribeVpcs` izin. Hal ini memungkinkan GuardDuty untuk melacak pembaruan VPC, seperti mengambil VPC CIDR.	Agustus 22, 2024

Ubah	Deskripsi	Tanggal

AmazonGuardDutyFullAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin yang memungkinkan Anda untuk meneruskan peran IAM GuardDuty saat Anda mengaktifkan Perlindungan Malware untuk S3.
	
	{
	"Sid": "AllowPassRoleToMalwareProtectionPlan",
	"Effect": "Allow",
	"Action": [
	"iam:PassRole"
	],
	"Resource": "arn:aws:iam::*:role/*",
	"Condition": {
	"StringEquals": {
	"iam:PassedToService": "malware-protection-plan.guardduty.amazonaws.com"
	}
	}
	}
		Juni 10, 2024

Ubah	Deskripsi	Tanggal
AmazonGuardDutyServiceRolePolicy— Memperbarui ke kebijakan yang ada.	Gunakan AWS Systems Manager tindakan untuk mengelola asosiasi SSM pada instans Amazon EC2 saat Anda mengaktifkan Pemantauan GuardDuty Runtime dengan agen otomatis untuk Amazon EC2. Saat konfigurasi agen GuardDuty otomatis dinonaktifkan, GuardDuty pertimbangkan hanya instans EC2 yang memiliki tag inklusi (`GuardDuty Managed :true`).	26 Maret 2024
AmazonGuardDutyServiceRolePolicy— Memperbarui ke kebijakan yang ada.	GuardDuty telah menambahkan izin baru - `organization:DescribeOrganization` untuk mengambil ID organisasi dari akun Amazon VPC bersama dan menetapkan kebijakan titik akhir Amazon VPC dengan ID organisasi.	Februari 9, 2024

Ubah	Deskripsi	Tanggal
AmazonGuardDutyMalwareProtectionServiceRolePolicy— Memperbarui ke kebijakan yang ada.	Perlindungan Malware untuk EC2 telah menambahkan dua izin - `GetSnapshotBlock` dan `ListSnapshotBlocks` untuk mengambil snapshot volume EBS (dienkripsi menggunakan Kunci yang dikelola AWS) dari Anda Akun AWS dan menyalinnya ke akun GuardDuty layanan sebelum memulai pemindaian malware.	25 Jan 2024
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan izin baru untuk memungkinkan GuardDuty untuk menambahkan pengaturan akun `guardduty Activate` Amazon ECS, dan melakukan daftar dan menjelaskan operasi pada cluster Amazon ECS.	26 November 2023
AmazonGuardDutyReadOnlyAccess – Pembaruan ke kebijakan yang ada	GuardDuty menambahkan kebijakan baru `organizations` untuk`ListAccounts` .	16 November 2023
AmazonGuardDutyFullAccess – Pembaruan ke kebijakan yang ada	GuardDuty menambahkan kebijakan baru `organizations` untuk`ListAccounts` .	16 November 2023

Ubah	Deskripsi	Tanggal
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	GuardDuty menambahkan izin baru untuk mendukung fitur GuardDuty EKS Runtime Monitoring yang akan datang.	8 Maret 2023
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	GuardDuty telah menambahkan izin baru untuk memungkinkan GuardDuty membuat Service-linked peran untuk Perlindungan Malware untuk EC2. Ini akan membantu GuardDuty meramping kan proses mengaktifkan Perlindungan Malware untuk EC2. GuardDuty sekarang dapat melakukan tindakan IAM berikut: `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	21 Februari 2023

Ubah	Deskripsi	Tanggal
AmazonGuardDutyFullAccess – Pembaruan ke kebijakan yang ada	GuardDuty ARN diperbarui `iam:GetRole` untuk `*AWSServiceRoleForAmazonGuardDutyMalwareProtection` .	Juli 26, 2022
AmazonGuardDutyFullAccess – Pembaruan ke kebijakan yang ada	GuardDuty menambahkan yang baru `AWSServiceName` untuk memungkinkan pembuatan peran terkait layanan menggunakan `iam:CreateServiceLinkedRole` untuk Perlindungan GuardDuty Malware untuk layanan EC2. GuardDuty sekarang dapat melakukan `iam:GetRole` tindakan untuk mendapatkan informasi`AWSServiceRole` .	Juli 26, 2022

Ubah	Deskripsi	Tanggal
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	GuardDuty menambahkan izin baru GuardDuty untuk memungkinkan penggunaan tindakan jaringan Amazon EC2 untuk meningkatkan temuan. GuardDuty sekarang dapat melakukan tindakan EC2 berikut untuk mendapatkan informasi tentang bagaimana instans EC2 Anda berkomunikasi. Informasi ini digunakan untuk meningkatkan akurasi temuan. • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	3 Agustus 2021
GuardDuty mulai melacak perubahan	GuardDuty mulai melacak perubahan untuk kebijakan yang AWS dikelolanya.	3 Agustus 2021

Memecahkan masalah GuardDuty identitas dan akses Amazon

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan GuardDuty dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di GuardDuty
- Saya tidak berwenang untuk melakukan iam:PassRole.
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses GuardDuty sumber daya saya.

Saya tidak berwenang untuk melakukan tindakan di GuardDuty

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `guardduty:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `guardduty:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam:PassRole.

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran GuardDuty.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di GuardDuty. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses GuardDuty sumber daya saya.

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah GuardDuty mendukung fitur ini, lihatBagaimana Amazon GuardDuty bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Validasi kepatuhan untuk Amazon GuardDuty

Pengalaman AWS pendaftaran baru kami tidak dirancang untuk beban kerja yang diatur. Jika Anda menggunakan pengalaman AWS pendaftaran baru kami, tetapi ingin menggunakannya AWS untuk beban kerja yang diatur, Anda dapat mendaftar untuk AWS (lanjutan) atau mengaktifkan fitur lanjutan untuk lingkungan Anda AWS .

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup berdasarkan Program Kepatuhan dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program Kep AWS atuhan Program Jaminan .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat Dokumentasi AWS Keamanan.

Ketahanan di Amazon GuardDuty

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat infrastruktur AWS global.

Keamanan infrastruktur di Amazon GuardDuty

Sebagai layanan terkelola, Amazon GuardDuty dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses GuardDuty melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.

- Cipher suite dengan perfect forward secrecy (PFS) seperti DHE (Ephemeral) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Amazon GuardDuty dan titik akhir VPC antarmuka ()AWS PrivateLink

Anda dapat membuat koneksi pribadi antara VPC dan Amazon GuardDuty dengan membuat antarmuka VPC endpoint. Endpoint antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda mengakses GuardDuty API secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi Direct AWS Connect. Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi GuardDuty dengan API. Lalu lintas antara VPC Anda dan GuardDuty tidak meninggalkan jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa Antarmuka Jaringan Elastis di subnet Anda.

Untuk informasi selengkapnya, lihat Titik akhir VPC Antarmuka (AWS PrivateLink) di Panduan.AWS PrivateLink

Pertimbangan untuk titik akhir GuardDuty VPC

Sebelum menyiapkan titik akhir VPC antarmuka GuardDuty, pastikan Anda meninjau properti dan batasan titik akhir Antarmuka dalam Panduan.AWS PrivateLink

GuardDuty mendukung panggilan ke semua tindakan API-nya dari VPC Anda.

Membuat titik akhir VPC antarmuka untuk GuardDuty

Anda dapat membuat titik akhir VPC untuk GuardDuty layanan menggunakan konsol VPC Amazon atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di AWS PrivateLink Panduan.

Buat titik akhir VPC untuk GuardDuty menggunakan nama layanan berikut:

- com.amazonaws. *region*.guardduty
- com.amazonaws. *region*.guardduty-fips (titik akhir FIPS)

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API untuk GuardDuty menggunakan nama DNS default untuk Wilayah, misalnya,. `guardduty.us-east-1.amazonaws.com`

Untuk informasi selengkapnya, lihat Mengakses layanan melalui titik akhir antarmuka di AWS PrivateLink Panduan.

Membuat kebijakan titik akhir VPC untuk GuardDuty

Anda dapat melampirkan kebijakan titik akhir ke VPC endpoint yang mengendalikan akses ke GuardDuty. Kebijakan titik akhir menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke layanan dengan titik akhir VPC di Panduan.AWS PrivateLink

Contoh: Kebijakan titik akhir VPC untuk tindakan GuardDuty

Berikut ini adalah contoh kebijakan endpoint untuk GuardDuty. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke GuardDuty tindakan yang tercantum untuk semua prinsipal di semua sumber daya.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "guardduty:listDetectors",
            "guardduty:getDetector",
            "guardduty:getFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

Subnet bersama

Anda tidak dapat membuat, mendeskripsikan, memodifikasi, atau menghapus titik akhir VPC di subnet yang dibagikan dengan Anda. Namun, Anda dapat menggunakan titik akhir VPC di subnet yang dibagikan dengan Anda. Untuk informasi tentang berbagi VPC, lihat Membagikan VPC Anda dengan akun lain di Panduan Pengguna Amazon VPC.

GuardDuty Integrasi dengan layanan AWS keamanan

GuardDuty dapat diintegrasikan dengan layanan AWS keamanan lainnya. Layanan ini dapat menyerap data dari GuardDuty untuk memungkinkan Anda melihat temuan dengan cara baru. Tinjau opsi integrasi berikut untuk mempelajari lebih lanjut tentang cara layanan tersebut disiapkan untuk bekerja dengannya GuardDuty.

Integrasi dengan GuardDuty AWS Security Hub CSPM

AWS Security Hub CSPM mengumpulkan data keamanan dari seluruh AWS akun, layanan, dan produk mitra pihak ketiga yang didukung untuk menilai keadaan keamanan lingkungan Anda sesuai dengan standar industri dan praktik terbaik. Selain mengevaluasi postur keamanan Anda, Security Hub CSPM menciptakan lokasi terpusat untuk temuan di semua AWS layanan terintegrasi Anda, dan AWS produk Mitra. Mengaktifkan Security Hub CSPM dengan GuardDuty akan secara otomatis memungkinkan data GuardDuty temuan dicerna oleh Security Hub CSPM.

Untuk informasi selengkapnya tentang menggunakan Security Hub CSPM dengan GuardDuty lihat. Integrasi dengan AWS Security Hub CSPM

Integrasi GuardDuty dengan Amazon Detective

Amazon Detective menggunakan data log dari seluruh AWS akun Anda untuk membuat visualisasi data untuk sumber daya dan alamat IP yang berinteraksi dengan lingkungan Anda. Visualisasi Detective membantu Anda menyelidiki masalah keamanan dengan cepat dan mudah. Anda dapat beralih dari GuardDuty menemukan detail ke informasi di konsol Detektif setelah kedua layanan diaktifkan.

Untuk informasi lebih lanjut tentang menggunakan Detektif dengan GuardDuty lihat. Integrasi dengan Amazon Detective

Integrasi dengan AWS Security Hub CSPM

AWS Security Hub CSPM memberi Anda gambaran menyeluruh tentang status keamanan Anda dalam AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub CSPM mengumpulkan data keamanan dari berbagai AWS akun, layanan, dan produk mitra pihak ketiga yang didukung serta membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi.

GuardDuty Integrasi Amazon dengan Security Hub CSPM memungkinkan Anda mengirim temuan GuardDuty ke Security Hub CSPM. Security Hub CSPM kemudian dapat memasukkan temuan-temuan tersebut dalam analisisnya tentang postur keamanan Anda.

Daftar Isi

- Bagaimana Amazon GuardDuty mengirimkan temuan ke AWS Security Hub CSPM
  - Jenis temuan yang GuardDuty dikirim ke Security Hub CSPM
    - Latensi untuk mengirimkan temuan baru
    - Mencoba lagi saat Security Hub CSPM tidak tersedia
    - Memperbarui temuan yang ada di Security Hub CSPM
- Melihat GuardDuty temuan di AWS Security Hub CSPM
  - Menafsirkan GuardDuty menemukan nama di AWS Security Hub CSPM
  - Temuan khas dari GuardDuty
- Mengaktifkan dan mengonfigurasi integrasi
- Menggunakan GuardDuty kontrol di Security Hub CSPM
- Menghentikan publikasi temuan ke Security Hub CSPM

Bagaimana Amazon GuardDuty mengirimkan temuan ke AWS Security Hub CSPM

Pada tahun AWS Security Hub CSPM, masalah keamanan dilacak sebagai temuan. Beberapa temuan berasal dari masalah yang terdeteksi oleh AWS layanan lain atau oleh mitra pihak ketiga. Security Hub CSPM juga memiliki seperangkat aturan yang digunakan untuk mendeteksi masalah keamanan dan menghasilkan temuan.

Security Hub CSPM menyediakan alat untuk mengelola temuan dari seluruh sumber ini. Anda dapat melihat dan mem-filter daftar temuan dan melihat detail suatu temuan. Untuk informasi lebih lanjut, lihat Melihat temuan dalam Panduan Pengguna AWS Security Hub . Anda juga dapat melacak status penyelidikan temuan. Untuk informasi lebih lanjut, lihat Mengambil tindakan pada temuan dalam Panduan Pengguna AWS Security Hub .

Semua temuan di Security Hub CSPM menggunakan format JSON standar yang disebut AWS Security Finding Format (ASFF). ASFF mencakup detail tentang sumber masalah, sumber daya yang terdampak, dan status temuan saat ini. Lihat AWS Security Finding Format (ASFF) di Panduan Pengguna AWS Security Hub .

Amazon GuardDuty adalah salah satu AWS layanan yang mengirimkan temuan ke Security Hub CSPM.

Jenis temuan yang GuardDuty dikirim ke Security Hub CSPM

Setelah Anda mengaktifkan GuardDuty dan Security Hub CSPM di akun yang sama dalam akun yang sama Wilayah AWS, GuardDuty mulai mengirimkan semua temuan yang dihasilkan ke Security Hub CSPM. Temuan ini dikirim ke Security Hub CSPM menggunakan AWS Security Finding Format (ASFF). Dalam ASFF, bidang `Types` menyediakan jenis temuan.

Latensi untuk mengirimkan temuan baru

Ketika GuardDuty membuat temuan baru, biasanya dikirim ke Security Hub CSPM dalam waktu lima menit.

Mencoba lagi saat Security Hub CSPM tidak tersedia

Jika Security Hub CSPM tidak tersedia, GuardDuty coba lagi mengirimkan temuan sampai diterima.

Memperbarui temuan yang ada di Security Hub CSPM

Setelah mengirimkan temuan ke Security Hub CSPM, GuardDuty mengirimkan pembaruan untuk mencerminkan pengamatan tambahan dari aktivitas temuan ke Security Hub CSPM. Pengamatan baru dari temuan ini dikirim ke Security Hub CSPM berdasarkan Langkah 5 — Frekuensi untuk mengekspor temuan pengaturan di Anda. Akun AWS

Saat Anda mengarsipkan atau membatalkan arsip temuan, GuardDuty tidak akan mengirimkan temuan itu ke Security Hub CSPM. Temuan yang tidak diarsipkan secara manual yang kemudian menjadi aktif tidak dikirim ke Security Hub CSPM. GuardDuty

Melihat GuardDuty temuan di AWS Security Hub CSPM

Masuk ke Konsol Manajemen AWS dan buka AWS Security Hub CSPM konsol di https://console.aws.amazon.com/securityhub/.

Anda sekarang dapat menggunakan salah satu cara berikut untuk melihat GuardDuty temuan di konsol CSPM Security Hub:

Opsi 1: Menggunakan Integrasi di Security Hub CSPM

1. Di panel navigasi kiri, pilih Integrasi.

2. Pada halaman Integrasi, periksa Status untuk Amazon: GuardDuty.
   - Jika Status Menerima temuan, maka pilih Lihat temuan di sebelah Menerima temuan.
   - Jika tidak, maka untuk informasi selengkapnya tentang cara kerja Integrasi, lihat Integrasi CSPM Security Hub di Panduan Pengguna.AWS Security Hub

Opsi 2: Menggunakan Temuan di Security Hub CSPM

1. Di panel navigasi kiri, pilih Temuan.
2. Pada halaman Temuan, tambahkan filter Nama produk dan masukkan **`GuardDuty`** untuk melihat hanya GuardDuty temuan.

Menafsirkan GuardDuty menemukan nama di AWS Security Hub CSPM

GuardDuty mengirimkan temuan ke Security Hub CSPM menggunakan AWS Security Finding Format (ASFF). Dalam ASFF, bidang `Types` menyediakan jenis temuan. Jenis ASFF menggunakan skema penamaan yang berbeda dari GuardDuty tipe. Tabel di bawah ini merinci semua jenis GuardDuty temuan dengan rekan ASFF mereka seperti yang muncul di Security Hub CSPM.

> **Note**
>
> Untuk beberapa jenis GuardDuty temuan Security Hub CSPM memberikan nama temuan ASFF yang berbeda tergantung pada apakah Peran Sumber Daya detail temuan adalah ACTOR atau TARGET. Untuk mengetahui informasi selengkapnya, lihat Detail temuan.

GuardDuty menemukan jenis	Tipe temuan ASFF
AttackSequence:IAM/CompromisedCredentials	TTPs/AttackSequence:IAM/CompromisedCredentials
AttackSequence:S3/CompromisedData	TTPs/AttackSequence:S3/CompromisedData
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS

GuardDuty menemukan jenis	Tipe temuan ASFF
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed

GuardDuty menemukan jenis	Tipe temuan ASFF
CredentialAccess:Kubernetes/MaliciousIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller.Custom
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	TTPs/CredentialAccess/CredentialAccess:Kubernetes-SuccessfulAnonymousAccess
CredentialAccess:Kubernetes/TorIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-TorIPCaller
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS

GuardDuty menemukan jenis	Tipe temuan ASFF
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CommandAndControl:Runtime/SuspiciousCommand	TTPs/Command and Control/CommandAndControl:Runtime-SuspiciousCommand
CredentialAccess:Runtime/SensitiveFileRead	TTPs/Credential Access/CredentialAccess:Runtime-SensitiveFileRead
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasion:IAMUser/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:IAMUser/BedrockLoggingDisabled	TTPs/Defense Evasion/DefenseEvasion:IAMUser-BedrockLoggingDisabled
DefenseEvasion:Kubernetes/MaliciousIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller.Custom

GuardDuty menemukan jenis	Tipe temuan ASFF
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-SuccessfulAnonymousAccess
DefenseEvasion:Kubernetes/TorIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-TorIPCaller
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/KernelModuleLoaded	TTPs/Defense Evasion/DefenseEvasion:Runtime-KernelModuleLoaded
DefenseEvasion:Runtime/SensitiveFileModified	TTPs/Defense Evasion/DefenseEvasion:Runtime-SensitiveFileModified
DefenseEvasion:Runtime/ProcessInjection.Proc	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Proc
DefenseEvasion:Runtime/ProcessInjection.Ptrace	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Ptrace
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.VirtualMemoryWrite
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand
Discovery:IAMUser/AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:Kubernetes/MaliciousIPCaller	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller

GuardDuty menemukan jenis	Tipe temuan ASFF
Discovery:Kubernetes/MaliciousIPCaller.Custom	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller.Custom
Discovery:Kubernetes/SuccessfulAnonymousAccess	TTPs/Discovery/Discovery:Kubernetes-SuccessfulAnonymousAccess
Discovery:Kubernetes/TorIPCaller	TTPs/Discovery/Discovery:Kubernetes-TorIPCaller
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:Runtime/SensitiveFileRead	TTPs/Discovery/Discovery:Runtime-SensitiveFileRead
Discovery:Runtime/SuspiciousCommand	TTPs/Discovery/Discovery:Runtime-SuspiciousCommand
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Exfiltration:IAMUser/AnomalousBehavior	TTPs/Exfiltration/IAMUser-AnomalousBehavior
Execution:Kubernetes/ExecInKubeSystemPod	TTPs/Execution/Execution:Kubernetes-ExecInKubeSystemPod
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod

GuardDuty menemukan jenis	Tipe temuan ASFF
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Impact:EC2/MaliciousDomainRequest.Custom	TTPs/Impact/Impact:EC2-MaliciousDomainRequest.Custom
Impact:Kubernetes/MaliciousIPCaller	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller
Impact:Kubernetes/MaliciousIPCaller.Custom	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller.Custom
Impact:Kubernetes/SuccessfulAnonymousAccess	TTPs/Impact/Impact:Kubernetes-SuccessfulAnonymousAccess
Impact:Kubernetes/TorIPCaller	TTPs/Impact/Impact:Kubernetes-TorIPCaller
Persistence:Kubernetes/ContainerWithSensitiveMount	TTPs/Persistence/Persistence:Kubernetes-ContainerWithSensitiveMount
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Persistence:Kubernetes/MaliciousIPCaller	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller
Persistence:Kubernetes/MaliciousIPCaller.Custom	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller.Custom
Persistence:Kubernetes/SuccessfulAnonymousAccess	TTPs/Persistence/Persistence:Kubernetes-SuccessfulAnonymousAccess

GuardDuty menemukan jenis	Tipe temuan ASFF
Persistence:Kubernetes/TorIPCaller	TTPs/Persistence/Persistence:Kubernetes-TorIPCaller
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:EC2/MaliciousFile!Snapshot	TTPs/Execution/Execution:EC2-MaliciousFile!Snapshot
Execution:EC2/MaliciousFile!AMI	TTPs/Execution/Execution:EC2-MaliciousFile!AMI
Execution:EC2/MaliciousFile!RecoveryPoint	TTPs/Execution/Execution:EC2-MaliciousFile!RecoveryPoint
Execution:S3/MaliciousFile!RecoveryPoint	TTPs/Execution/Execution:S3-MaliciousFile!RecoveryPoint
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted

GuardDuty menemukan jenis	Tipe temuan ASFF
Execution:Runtime/MaliciousFileExecuted.Custom	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted.Custom
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousShellCreated	TTPs/Execution/Execution:Runtime-SuspiciousShellCreated
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep

GuardDuty menemukan jenis	Tipe temuan ASFF
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
Impact:IAMUser/AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Exfiltration:Runtime/SuspiciousCommand	TTPs/Exfiltration/Exfiltration:Runtime-SuspiciousCommand
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller

GuardDuty menemukan jenis	Tipe temuan ASFF
InitialAccess:IAMUser/AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
Object:S3/MaliciousFile	TTPs/Object/Object:S3-MaliciousFile
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
Persistence:IAMUser/AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Persistence:Runtime/SuspiciousCommand	TTPs/Persistence/Persistence:Runtime-SuspiciousCommand
Persistence:Runtime/SensitiveFileModified	TTPs/Persistence/Persistence:Runtime-SensitiveFileModified
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:IAMUser/ShortTermRootCredentialUsage	TTPs/Policy:IAMUser-ShortTermRootCredentialUsage

GuardDuty menemukan jenis	Tipe temuan ASFF
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AdminAccessToDefaultServiceAccount
Policy:Kubernetes/AnonymousAccessGranted	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AnonymousAccessGranted
Policy:Kubernetes/ExposedDashboard	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-ExposedDashboard
Policy:Kubernetes/KubeflowDashboardExposed	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-KubeflowDashboardExposed
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation:IAMUser/AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleBindingCreated

GuardDuty menemukan jenis	Tipe temuan ASFF
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Kubernetes/PrivilegedContainer	TTPs/PrivilegeEscalation/PrivilegeEscalation:Kubernetes-PrivilegedContainer
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/ElevationToRoot	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ElevationToRoot
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
PrivilegeEscalation:Runtime/SuspiciousCommand	Software and Configuration Checks/PrivilegeEscalation:Runtime-SuspiciousCommand
PrivilegeEscalation:Runtime/SensitiveFileModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-SensitiveFileModified
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan

GuardDuty menemukan jenis	Tipe temuan ASFF
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS

GuardDuty menemukan jenis	Tipe temuan ASFF
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS

GuardDuty menemukan jenis	Tipe temuan ASFF
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/UnauthorizedAccess:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS

GuardDuty menemukan jenis	Tipe temuan ASFF
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-ResourceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-ResourceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay

GuardDuty menemukan jenis	Tipe temuan ASFF
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

Temuan khas dari GuardDuty

GuardDuty mengirimkan temuan ke Security Hub CSPM menggunakan AWS Security Finding Format (ASFF).

Berikut adalah contoh temuan khas dari GuardDuty.


```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws:securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356.",
```

```
  "Description": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
 instance by guessing the SSH password.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
 "Unknown",
    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
 "199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
 "46717",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
 "172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
 "INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
 "SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
```

```
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/guardduty/
arn:aws:guardduty:us-east-1:193043430472:detector/d4b040365221be2b54a6264dc9a4bc64/
finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```

Mengaktifkan dan mengonfigurasi integrasi

Untuk menggunakan integrasi dengan AWS Security Hub CSPM, Anda harus mengaktifkan Security Hub CSPM. Untuk informasi tentang cara mengaktifkan CSPM Security Hub, lihat Menyiapkan Security Hub di AWS Security Hub Panduan Pengguna.

Ketika Anda mengaktifkan keduanya GuardDuty dan Security Hub CSPM, integrasi diaktifkan secara otomatis. GuardDutysegera mulai mengirim temuan ke Security Hub CSPM.

Menggunakan GuardDuty kontrol di Security Hub CSPM

AWS Security Hub CSPM menggunakan kontrol keamanan untuk mengevaluasi AWS sumber daya Anda, dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Anda dapat menggunakan kontrol yang terkait dengan GuardDuty sumber daya dan rencana perlindungan yang dipilih. Untuk informasi selengkapnya, lihat GuardDutykontrol Amazon di Panduan AWS Security Hub Pengguna.

Untuk daftar semua kontrol di seluruh AWS layanan dan sumber daya, lihat Referensi kontrol CSPM Security Hub di AWS Security Hub Panduan Pengguna.

Menghentikan publikasi temuan ke Security Hub CSPM

Untuk menghentikan pengiriman temuan ke Security Hub CSPM, Anda dapat menggunakan konsol CSPM Security Hub atau API.

Lihat Menonaktifkan dan mengaktifkan alur temuan dari integrasi (konsol) atau Menonaktifkan alur temuan dari integrasi (Security Hub API, AWS CLI) di Panduan Pengguna.AWS Security Hub

Integrasi dengan Amazon Detective

Amazon Detective membantu Anda menganalisis dan menyelidiki peristiwa keamanan dengan cepat di satu atau beberapa AWS akun dengan menghasilkan visualisasi data yang mewakili cara sumber daya Anda berperilaku dan berinteraksi dari waktu ke waktu. Detective menciptakan visualisasi temuan. GuardDuty

Detective menyerap rincian pencarian untuk semua jenis temuan, dan menyediakan akses ke profil entitas untuk menyelidiki entitas berbeda yang terlibat dengan temuan tersebut. Entitas dapat berupa Akun AWS, AWS sumber daya dalam akun, atau Alamat IP eksternal yang telah berinteraksi dengan

sumber daya Anda. GuardDuty Konsol mendukung pivoting ke Amazon Detective dari entitas berikut, tergantung pada jenis pencarian:, peran IAM, pengguna Akun AWS, atau sesi peran, agen pengguna, pengguna federasi, instans Amazon EC2, atau alamat IP.

Daftar Isi

- Mengaktifkan integrasi
- Berputar ke Detektif Amazon dari sebuah temuan GuardDuty
- Menggunakan integrasi dengan lingkungan GuardDuty multi-akun

Mengaktifkan integrasi

Untuk menggunakan Amazon Detective dengan GuardDuty Anda harus terlebih dahulu mengaktifkan Amazon Detective. Untuk informasi tentang cara mengaktifkan Detektif, lihat Memulai Detektif Amazon di Panduan Pengguna Detektif Amazon.

Saat Anda mengaktifkan keduanya GuardDuty dan Detektif, integrasi diaktifkan secara otomatis. Setelah diaktifkan, Detektif akan segera menelan data temuan Anda GuardDuty .

> **Note**
>
> GuardDuty mengirimkan temuan ke Detective berdasarkan frekuensi ekspor GuardDuty temuan. Secara default, frekuensi ekspor untuk pembaruan temuan yang ada adalah 6 jam. Untuk memastikan Detektif menerima pembaruan terbaru untuk temuan Anda, disarankan agar Anda mengubah frekuensi ekspor menjadi 15 menit di setiap wilayah tempat Anda menggunakan Detektif. GuardDuty Untuk mengetahui informasi selengkapnya, lihat Langkah 5 - Mengatur frekuensi untuk mengekspor temuan aktif yang diperbarui.

Berputar ke Detektif Amazon dari sebuah temuan GuardDuty

1. Masuk ke https://console.aws.amazon.com/guardduty/konsol.
2. Pilih satu temuan dari tabel temuan Anda.
3. Pilih Selidiki dengan Detektif dari panel rincian temuan.
4. Pilih aspek temuan untuk diselidiki dengan Amazon Detective. Konsol Detective akan terbuka untuk temuan atau entitas tersebut.

Jika pivot tidak berperilaku seperti yang diharapkan, lihat Memecahkan masalah pivot di Panduan Pengguna Detektif Amazon.

> **Note**
>
> Jika Anda mengarsipkan GuardDuty temuan di konsol Detektif, temuan itu akan diarsipkan di GuardDuty konsol juga.

Menggunakan integrasi dengan lingkungan GuardDuty multi-akun

Jika Anda mengelola lingkungan multi-akun di GuardDuty, Anda harus menambahkan akun anggota Anda ke Amazon Detective untuk melihat visualisasi data Detektif untuk temuan dan entitas di akun tersebut.

Disarankan agar Anda menggunakan akun GuardDuty Administrator yang sama dengan akun administrator untuk Detektif. Untuk informasi selengkapnya tentang menambahkan akun anggota di Detektif, lihat Mengelola akun di Panduan Pengguna Detektif Amazon.

> **Note**
>
> Detective adalah layanan regional. Artinya, Anda harus mengaktifkan Detective dan menambahkan akun anggota Anda di setiap wilayah tempat Anda ingin menggunakan integrasi.

Menangguhkan atau menonaktifkan GuardDuty

Anda dapat menggunakan GuardDuty konsol untuk menangguhkan atau menonaktifkan GuardDuty layanan. Anda tidak dikenakan biaya untuk menggunakan GuardDuty ketika layanan ditangguhkan.

- Semua akun anggota harus dipisahkan atau dihapus sebelum Anda dapat menangguhkan atau menonaktifkan. GuardDuty
- Jika Anda menangguhkan GuardDuty, itu tidak lagi memantau keamanan AWS lingkungan Anda atau menghasilkan temuan baru. Temuan Anda yang ada tetap utuh dan tidak terpengaruh oleh GuardDuty penangguhan. Anda dapat memilih untuk mengaktifkan kembali GuardDuty nanti.
- Ketika Anda menonaktifkan GuardDuty di akun, itu akan dinonaktifkan hanya untuk yang saat ini dipilih Wilayah AWS. Jika Anda ingin menonaktifkan sepenuhnya GuardDuty, Anda harus menonaktifkannya di setiap Wilayah tempat diaktifkan.
- Jika Anda menonaktifkan GuardDuty, temuan Anda yang ada dan GuardDuty konfigurasi hilang dan tidak dapat dipulihkan. Jika Anda ingin menyimpan temuan yang ada, Anda harus mengekspornya sebelum mengonfirmasi untuk menonaktifkan GuardDuty. Untuk informasi tentang cara mengekspor temuan, lihatMengekspor temuan yang dihasilkan ke Amazon S3.
- Jika Anda telah mengaktifkan Perlindungan Malware untuk S3 untuk satu atau beberapa bucket yang dilindungi di akun Anda, maka menangguhkan atau menonaktifkan GuardDuty tidak memengaruhi status bucket yang dilindungi di bawah Perlindungan Malware untuk S3. Bahkan setelah menangguhkan atau menonaktifkan GuardDuty, akun Anda akan terus mengeluarkan biaya penggunaan yang terkait dengan fitur Perlindungan Malware untuk S3. Untuk informasi tentang menonaktifkan Perlindungan Malware untuk S3, lihat. Menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi

Untuk menangguhkan atau menonaktifkan GuardDuty

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di GuardDuty bagian Tangguhkan, pilih Tangguhkan GuardDuty atau Nonaktifkan GuardDuty, lalu Konfirmasikan tindakan Anda.

Untuk mengaktifkan kembali GuardDuty setelah menangguhkan

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.

2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih Re-enable GuardDuty.

Berlangganan pengumuman Amazon GuardDuty SNS

Bagian ini memberikan informasi tentang berlangganan Amazon SNS (Layanan Pemberitahuan Sederhana) GuardDuty untuk pengumuman untuk menerima pemberitahuan tentang jenis temuan yang baru dirilis, pembaruan untuk jenis temuan yang ada, dan perubahan fungsionalitas lainnya. Notifikasi tersedia dalam semua format yang didukung Amazon SNS.

GuardDuty SNS mengirimkan pengumuman tentang pembaruan ke GuardDuty layanan di seluruh AWS akun berlangganan apa pun. Untuk menerima pemberitahuan tentang temuan dalam akun Anda, lihatMemproses GuardDuty temuan dengan Amazon EventBridge.

> **Note**
>
> Pengguna IAM Anda harus memiliki `sns::subscribe` izin untuk berlangganan SNS.

Anda dapat berlangganan antrean Amazon SQS untuk topik notifikasi ini, tetapi Anda harus menggunakan ARN topik yang berada di Wilayah yang sama. Untuk informasi selengkapnya, lihat Tutorial: Berlangganan antrian Amazon SQS ke topik Amazon SNS di panduan pengembang Amazon Simple Queue Service.

Anda juga dapat menggunakan AWS Lambda fungsi untuk memicu peristiwa saat pemberitahuan diterima. Untuk informasi selengkapnya, lihat Memanggil fungsi Lambda menggunakan notifikasi Amazon SNS di panduan pengembang Layanan Antrian Sederhana Amazon.

ARN topik Amazon SNS untuk setiap Wilayah ditunjukkan di bawah ini.

Wilayah AWS	ARN topik Amazon SNS
US East (N. Virginia) - `us-east-1`	`arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements`
AS Timur (Ohio) - `us-east-2`	`arn:aws:sns:us-east-2:118283430703:GuardDutyAnnouncements`

Wilayah AWS	ARN topik Amazon SNS
AS Barat (California N.) - us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
US West (Oregon) - us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
Kanada (Tengah) - ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
Kanada Barat (Calgary) - ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
Eropa (Stockholm) - eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
Eropa (Irlandia) - eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements
Eropa (London) - eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements

Wilayah AWS	ARN topik Amazon SNS
Eropa (Paris) - `eu-west-3`	`arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements`
Eropa (Frankfurt) - `eu-central-1`	`arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements`
Eropa (Zurich) - `eu-central-2`	`arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements`
Asia Pasifik (Hong Kong) - `ap-east-1`	`arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements`
Asia Pacific (Tokyo) - `ap-northeast-1`	`arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements`
Asia Pasifik (Seoul) - `ap-northeast-2`	`arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements`
Asia Pasifik (Singapura) - `ap-southeast-1`	`arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements`

Wilayah AWS	ARN topik Amazon SNS
Asia Pasifik (Sydney) - ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
Asia Pasifik (Mumbai) - ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
Amerika Selatan (São Paulo) - sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
AWS GovCloud (US-West) - us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
Tiongkok (Beijing) - cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
Tiongkok (Ningxia) - cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements
Timur Tengah (Bahrain) - me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements

Wilayah AWS	ARN topik Amazon SNS
Timur Tengah (UEA) - me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
Eropa (Milan) - eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
Eropa (Spanyol) - eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
AWS GovCloud (US-East) - us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
Asia Pasifik (Osaka) - ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
Asia Pasifik (Jakarta) - ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements
Asia Pasifik (Hyderabad) - ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements

Wilayah AWS	ARN topik Amazon SNS
Asia Pasifik (Melbourne) - `ap-southeast-4`	`arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements`
Asia Pasifik (Malaysia) - `ap-southeast-5`	`arn:aws:sns:ap-southeast-5:343218181797:GuardDutyAnnouncements`
Israel (Tel Aviv) - `il-central-1`	`arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements`
Asia Pasifik (Thailand) - `ap-southeast-7`	`arn:aws:sns:ap-southeast-7:863518448376:GuardDutyAnnouncements`
Meksiko (Tengah) - `mx-central-1`	`arn:aws:sns:mx-central-1:060795916546:GuardDutyAnnouncements`
Asia Pasifik (Taipei) - `ap-east-2`	`arn:aws:sns:ap-east-2:604225987917:GuardDutyAnnouncements`

Untuk berlangganan email pemberitahuan GuardDuty pembaruan di Konsol Manajemen AWS

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Dalam daftar Wilayah, pilih Wilayah yang sama dengan ARN topik yang akan dijadikan langganan. Contoh ini menggunakan Wilayah `us-west-2`.

3. Di sebelah kiri panel navigasi, pilih Berlangganan, Buat berlangganan.
4. Pada kotak dialog Buat Langganan, untuk ARN Topik, tempel ARN topik: `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. Untuk Protokol, pilih Email. Untuk Titik Akhir, ketik alamat email yang bisa Anda gunakan untuk menerima notifikasi.
6. Pilih Buat langganan.
7. Di aplikasi email Anda, buka pesan dari AWS Pemberitahuan dan buka tautan untuk mengonfirmasi langganan Anda.

   Browser web Anda menampilkan respons konfirmasi dari Amazon SNS.

Untuk berlangganan email pemberitahuan GuardDuty pembaruan dengan AWS CLI

1. Jalankan perintah berikut dengan AWS CLI:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Di aplikasi email Anda, buka pesan dari AWS Pemberitahuan dan buka tautan untuk mengonfirmasi langganan Anda.

   Browser web Anda menampilkan respons konfirmasi dari Amazon SNS.

Format pesan Amazon SNS

Contoh pesan pemberitahuan GuardDuty umum:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"GENERAL\",\"message\":[{\"title\":
\"Updated AmazonGuardDutyFullAccess_v2 policy\",\"body\":\"Added permission that
 allows you to pass an IAM role to GuardDuty when you enable Malware Protection for
 S3.\",\"links\":[\"https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess-v2\"]}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
```

```
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:

```
{
        "version": "1",
        "type": "GENERAL",
        "message": [
            {
                "title": "Updated AmazonGuardDutyFullAccess policy",
                "body": "Added permission that allows you to pass an IAM role to
 GuardDuty when you enable Malware Protection for S3.",
                "links": [
                    "https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess-v2"
                ]
             }
        ]
}
```

Contoh pesan pemberitahuan GuardDuty pembaruan tentang temuan baru ditunjukkan di bawah ini:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
 environment is making connections to a Tor Guard or an Authority node. Tor is software
```

```
 for enabling anonymous communication. Tor Guards and Authority nodes act as initial
 gateways into a Tor network. This traffic can indicate that this EC2 instance is
 acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised.\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:

```
{
    "version": "1",
    "type": "NEW_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "findingDescription": "This finding informs you that an EC2 instance in your
 AWS environment is making connections to a Tor Guard or an Authority node. Tor is
 software for enabling anonymous communication. Tor Guards and Authority nodes act as
 initial gateways into a Tor network. This traffic can indicate that this EC2 instance
 is acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised."
    }]
}
```

Contoh pesan pemberitahuan GuardDuty pembaruan tentang pembaruan GuardDuty fungsionalitas ditunjukkan di bawah ini:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails
\":[{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
 events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_controlplane\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:

```
{
    "version": "1",
    "type": "NEW_FEATURES",
    "featureDetails": [{
        "featureDescription": "Customers with high-volumes of global CloudTrail events
 should see a net positive impact on their GuardDuty costs.",
        "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_controlplane"
    }]
}
```

Contoh pesan pemberitahuan GuardDuty pembaruan tentang temuan yang diperbarui ditunjukkan di bawah ini:

```
{
    "Type": "Notification",
```

```
    "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"description\":\"Increased severity value from 5 to 8.\"}]}",
    "Timestamp": "2018-03-09T00:25:43.483Z",
    "SignatureVersion": "1",
    "Signature": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```


Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:

```
{
    "version": "1",
    "type": "UPDATED_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "description": "Increased severity value from 5 to 8."
    }]
}
```

GuardDuty Kuota Amazon

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk masing-masing. Layanan AWS Kecuali dinyatakan lain, setiap kuota adalah Region-specific. Anda dapat meminta kenaikan untuk beberapa kuota, dan kuota lainnya tidak dapat ditingkatkan.

Untuk melihat kuota GuardDuty, buka konsol Service Quotas. Di panel navigasi, pilih Layanan AWSdan pilih Amazon GuardDuty.

Untuk meminta penambahan kuota, lihat Meminta penambahan kuota di Panduan Pengguna Service Quotas.

Anda Akun AWS memiliki kuota berikut untuk Amazon GuardDuty per Wilayah.

> **Note**
>
> - Untuk kuota khusus untuk Perlindungan GuardDuty Malware untuk EC2, lihat. Kuota dalam Perlindungan Malware untuk EC2
> - Untuk kuota khusus untuk Perlindungan Malware untuk S3, lihat. Kuota dalam Perlindungan Malware untuk S3

GuardDuty kuota per Wilayah

Sumber daya	Default	Komentar
Detektor	1	Jumlah maksimum sumber daya detektor yang dapat Anda buat per akun AWS per Wilayah. Anda tidak dapat meminta kenaikan kuota.
Penyaring	100	Jumlah maksimum filter yang disimpan

Sumber daya	Default	Komentar
		per AWS akun per Wilayah. Anda tidak dapat meminta kenaikan kuota.
Menemukan periode retensi	90 hari	Jumlah maksimum hari temuan dipertahankan. Anda tidak dapat meminta kenaikan kuota.
Alamat IP dan rentang CIDR per daftar alamat IP tepercaya	2.000	Jumlah maksimum alamat IP dan rentang CIDR yang dapat Anda sertakan dalam satu daftar alamat IP tepercaya. Anda tidak dapat meminta kenaikan kuota.
Alamat IP dan rentang CIDR per daftar alamat IP ancaman	250.000	Jumlah maksimum alamat IP dan rentang CIDR yang dapat Anda sertakan dalam daftar alamat IP ancaman. Anda tidak dapat meminta kenaikan kuota.

Sumber daya	Default	Komentar
Entitas per daftar entitas ancaman	1.000	Jumlah maksimum entitas yang dapat Anda sertakan dalam satu daftar entitas ancaman. Anda tidak dapat meminta kenaikan kuota.
Entitas per daftar entitas tepercaya	1.000	Jumlah maksimum entitas yang dapat Anda sertakan dalam daftar entitas tepercaya. Anda tidak dapat meminta kenaikan kuota.
Ukuran file maksimum	35 MB	Ukuran file maksimum untuk file yang digunakan untuk mengunggah daftar entitas atau daftar alamat IP. Anda tidak dapat meminta kenaikan kuota.

Sumber daya	Default	Komentar
Akun anggota (dengan undangan)	5000	Jumlah maksimum akun anggota yang terkait dengan akun administrator. Anda tidak dapat meminta kenaikan kuota.

Sumber daya	Default	Komentar
Akun anggota	50.000	Jumlah maksimum akun anggota yang terkait dengan akun administrator melalui AWS Organizat ions. Ini termasuk akun anggota yang ditambahkan ke organisasi melalui undangan. Nilai default ini tergantung pada kuota Anda saat ini untuk akun anggota di AWS Organizat ions. Jumlah akun anggota GuardDuty yang ditambahkan tidak AWS Organizat ions dapat melebihi jumlah akun anggota di organisasi Anda. Untuk informasi tentang jumlah Akun AWS dalam organisas i, lihat Nilai maksimum dan minimum dalam Panduan AWS Organizations Pengguna.

Sumber daya	Default	Komentar
Ancaman intel set (daftar alamat IP)	6	Jumlah maksimum daftar alamat IP ancaman yang dapat Anda tambahkan Akun AWS per Wilayah. Anda tidak dapat meminta kenaikan kuota.
Set IP tepercaya (daftar alamat IP)	1	Jumlah maksimum daftar alamat IP tepercaya yang dapat diunggah dan diaktifkan Akun AWS per Wilayah. Anda tidak dapat meminta kenaikan kuota.
Daftar entitas ancaman	6	Jumlah maksimum daftar entitas ancaman yang dapat Anda tambahkan Akun AWS per Wilayah. Anda tidak dapat meminta kenaikan kuota.

Sumber daya	Default	Komentar
Daftar entitas tepercaya	1	Jumlah maksimum daftar entitas tepercaya yang dapat diunggah dan diaktifkan Akun AWS per Wilayah. Anda tidak dapat meminta kenaikan kuota.

GuardDuty Support Instans Terkelola

Tabel berikut menunjukkan dukungan yang GuardDuty dimiliki berbagai fitur untuk berbagai jenis instance terkelola.

Jenis Fitur Terkelola	Dukungan Runtime Monitoring	Perlindungan Malware untuk dukungan EC2
Mode Otomatis Amazon EKS	Didukung	Didukung
Instans AWS Fargate Dikelola Amazon ECS	Tidak didukung	Didukung
Instans Terkelola Lambda	Tidak didukung	Tidak didukung

Memecahkan Masalah Amazon GuardDuty

Saat Anda menerima masalah yang terkait dengan melakukan tindakan khusus GuardDuty, lihat topik di bagian ini.

Topik

- Mengekspor temuan ke Amazon S3 - kesalahan akses
- Perlindungan Malware untuk masalah EC2
- Masalah Pemantauan Runtime
- Masalah pemecahan masalah lainnya

Mengekspor temuan ke Amazon S3 - kesalahan akses

Saat Anda mengekspor GuardDuty temuan ke bucket Amazon S3 (tujuan penerbitan), jika GuardDuty tidak dapat mengakses tujuan penerbitan ini, Anda mungkin mendapatkan kesalahan akses.

Setelah Anda mengonfigurasi pengaturan untuk mengekspor temuan, jika GuardDuty tidak dapat mengekspor temuan, akan menampilkan pesan kesalahan pada halaman Pengaturan di GuardDuty konsol. Ini berpotensi terjadi ketika tidak GuardDuty dapat lagi mengakses sumber daya target. Misalnya, jika bucket Amazon S3 Anda telah dihapus atau izin untuk mengakses bucket diubah. Ini juga berpotensi terjadi ketika tidak GuardDuty dapat lagi mengakses AWS KMS kunci yang digunakan untuk mengenkripsi data di bucket Amazon S3 Anda. Ketika GuardDuty tidak dapat mengekspor, ia mengirimkan pemberitahuan ke email yang terkait dengan akun untuk memberikan informasi tentang masalah ini.

Bagaimana cara mengatasi kesalahan akses?

Untuk mengatasi masalah ini, pastikan sumber daya yang sesuai ada dan GuardDuty memiliki izin untuk mengakses sumber daya yang diperlukan.

Untuk informasi selengkapnya, lihat Mengekspor temuan yang dihasilkan ke Amazon S3.

Apa yang terjadi jika Anda tidak menyelesaikan kesalahan ini?

Jika Anda tidak menyelesaikan masalah sebelum periode retensi temuan 90 hari selesai GuardDuty, temuan Anda tidak akan diekspor. GuardDuty akan menonaktifkan pencarian pengaturan ekspor untuk akun ini di Wilayah tertentu.

Untuk mulai mengekspor temuan lagi, perbarui pengaturan konfigurasi di Wilayah tertentu.

Perlindungan Malware untuk masalah EC2

Bagian ini mencantumkan kesalahan yang mungkin Anda alami saat menyiapkan atau menggunakan Perlindungan Malware untuk EC2.

Hilang diperlukan AWS Organizations izin manajemen saat mengaktifkan pemindaian GuardDuty-initiated malware

Ketika Anda ingin mengelola beberapa akun dengan menggunakan AWS Organizations dan Anda mendapatkan kesalahan ini — `The request failed because you do not have the required AWS Organizations management account permission.` maka Anda kehilangan izin untuk mengaktifkan pemindaian GuardDuty-initiated malware untuk beberapa akun di organisasi Anda.

Untuk informasi tentang memberikan izin ke akun manajemen, lihatMembangun akses tepercaya untuk mengaktifkan pemindaian GuardDuty-initiated malware.

Saya memulai pemindaian On-demand malware tetapi menghasilkan kesalahan izin yang diperlukan hilang.

Jika Anda menerima kesalahan yang menunjukkan bahwa Anda tidak memiliki izin yang diperlukan untuk memulai pemindaian On-demand malware pada instans Amazon EC2, verifikasi bahwa Anda telah melampirkan kebijakan AWS kebijakan yang dikelola: AmazonGuardDutyFullAccess_v2 (direkomendasikan) tersebut ke peran IAM Anda.

Jika Anda anggota AWS organisasi dan masih menerima kesalahan yang sama, sambungkan dengan akun manajemen Anda. Untuk informasi selengkapnya, lihat AWS Organizations SCP — Akses ditolak.

Saya menerima GetRole kesalahan **`iam:`** saat bekerja dengan Perlindungan Malware untuk EC2.

Jika Anda menerima kesalahan ini —`Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection`, itu berarti Anda kehilangan izin untuk mengaktifkan pemindaian GuardDuty-initiated malware atau menggunakan pemindaian

On-demand malware. Verifikasi bahwa Anda telah melampirkan AWS kebijakan yang dikelola: AmazonGuardDutyFullAccess_v2 (direkomendasikan) kebijakan ke peran IAM Anda.

Saya adalah akun GuardDuty administrator yang perlu mengaktifkan pemindaian GuardDuty-initiated malware tetapi tidak menggunakan AWS kebijakan terkelola: AmazonGuardDutyFullAccess untuk mengelola GuardDuty.

- Konfigurasikan peran IAM yang Anda gunakan GuardDuty untuk memiliki izin yang diperlukan untuk mengaktifkan pemindaian GuardDuty-initiated malware. Untuk informasi selengkapnya tentang izin yang diperlukan, lihat Membuat peran terkait layanan untuk Perlindungan Malware untuk EC2.
- Lampirkan AWS kebijakan yang dikelola: AmazonGuardDutyFullAccess_v2 (direkomendasikan) ke peran IAM Anda. Ini akan membantu Anda mengaktifkan pemindaian GuardDuty-initiated malware untuk akun anggota.

Masalah Pemantauan Runtime

Bagian ini mencantumkan kesalahan yang mungkin Anda alami saat menyiapkan atau menggunakan Runtime Monitoring.

Masalah cakupan runtime

Ketika cakupan runtime dari sumber daya yang dilindungi Anda menjadi Tidak Sehat, GuardDuty konsol menyediakan jenis masalah yang tepat. Setelah Anda memiliki jenis masalah, gunakan dokumen berikut untuk melihat langkah pemecahan masalah untuk setiap jenis sumber daya yang didukung:

- Memecahkan masalah cakupan runtime Amazon EC2
- Memecahkan masalah cakupan ECS-Fargate runtime Amazon
- Memecahkan masalah cakupan runtime Amazon EKS

Memecahkan masalah kesalahan memori di Runtime Monitoring (hanya mendukung Amazon EC2)

Bagian ini menyediakan langkah-langkah pemecahan masalah ketika Anda mengalami kesalahan kehabisan memori berdasarkan CPU dan batas memori untuk menyebarkan agen GuardDuty keamanan secara manual.

Jika `systemd` menghentikan GuardDuty agen karena `out-of-memory` masalah dan Anda mengevaluasi bahwa memberikan lebih banyak memori kepada GuardDuty agen masuk akal, Anda dapat memperbarui batasnya.

1. Dengan izin root, buka`/lib/systemd/system/amazon-guardduty-agent.service`.
2. Temukan `MemoryLimit` dan`MemoryMax`, dan perbarui kedua nilainya.

```
MemoryLimit=256M
MemoryMax=256M
```

3. Setelah memperbarui nilai, restart GuardDuty agen dengan menggunakan perintah berikut:

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Jalankan perintah berikut untuk melihat status:

```
sudo systemctl status amazon-guardduty-agent
```

   Output yang diharapkan akan menunjukkan batas memori baru:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Saya AWS Step Functions alur kerja gagal secara tak terduga

Jika GuardDuty kontainer berkontribusi pada kegagalan alur kerja, lihatMemecahkan masalah cakupan ECS-Fargate runtime Amazon. Jika masalah berlanjut, maka untuk mencegah kegagalan alur kerja karena GuardDuty penampung, lakukan salah satu langkah berikut:

- Tambahkan `false` tag`GuardDutyManaged`: ke cluster Amazon ECS terkait.
- Nonaktifkan konfigurasi agen otomatis untuk AWS Fargate (khusus ECS) di tingkat akun. Tambahkan tag inklusi`GuardDutyManaged`: `true` ke cluster Amazon ECS terkait yang ingin Anda lanjutkan pemantauan dengan agen GuardDuty otomatis.

Masalah pemecahan masalah lainnya

Jika Anda tidak menemukan skenario yang sesuai dengan masalah Anda, lihat opsi pemecahan masalah berikut:

- Untuk masalah IAM umum saat Anda mengakses https://console.aws.amazon.com/guardduty/, lihatMemecahkan masalah GuardDuty identitas dan akses Amazon.
- Untuk masalah autentikasi dan otorisasi saat Anda mengakses AWS AWS Console Home, lihat Memecahkan Masalah IAM.

GuardDuty Wilayah Amazon dan titik akhir

Untuk melihat di Wilayah AWS mana Amazon GuardDuty tersedia, lihat GuardDuty titik akhir Amazon di. Referensi Umum Amazon Web Services

Kami menyarankan Anda mengaktifkan semua GuardDuty yang didukung Wilayah AWS. Hal ini memungkinkan GuardDuty untuk menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa bahkan di Wilayah yang tidak Anda gunakan secara aktif. Ini juga memungkinkan GuardDuty untuk memantau AWS CloudTrail peristiwa yang didukung Wilayah AWS, kemampuannya untuk mendeteksi aktivitas yang melibatkan layanan global berkurang.

Region-specific ketersediaan fitur

Daftar perbedaan regional untuk menentukan ketersediaan GuardDuty fitur.

Bidang yang dapat disaring diperluas untuk dan CreateFilter UpdateFilter

> Bidang tambahan yang dapat disaring untuk aturan dan filter penekanan hanya tersedia di AWS partisi (). `aws` Di partisi lain, Anda dapat terus menggunakan bidang yang didukung konsol.

ListFindings dan GetFindingsStatistics API

> ListFindingsAPI GetFindingsStatisticsdan memiliki `consoleOnly` bendera sementara. Bila Anda menggunakan salah satu atau kedua API ini, `consoleOnly` tanda berarti API dapat mengambil hasil hingga batas maksimum 1000.

Perlindungan Malware untuk EC2

> GuardDuty mendukung Perlindungan Malware untuk EC2 fitur di AWS Dedicated Local Zones.

Perlindungan RDS

> Perlindungan RDS tidak didukung di Wilayah Asia Pasifik (Taipei) (`ap-east-2`).
>
> Perlindungan RDS tidak didukung di Local Zones AWS Khusus.

Jenis temuan IAM — CredentialAccess:IAMUser/CompromisedCredentials

> Jenis CredentialAccess:IAMUser/CompromisedCredentials temuan tidak didukung di wilayah berikut.

Wilayah AWS	Kode Wilayah
AWS GovCloud (US-West)	us-gov-west-1
AWS GovCloud (US-East)	us-gov-east-1
Tiongkok (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1

Jenis temuan IAM — DefenseEvasion:IAMUser/BedrockLoggingDisabled

Jenis DefenseEvasion:IAMUser/BedrockLoggingDisabled temuan tidak didukung di Wilayah Asia Pasifik (Hong Kong) (`ap-east-1`).

Jenis penemuan Perlindungan AI

Jenis Impact:IAMUser/AnomalousModelInvocation dan Impact:IAMUser/CostHarvesting temuan membutuhkan Amazon Bedrock atau Amazon SageMaker AI. Di Wilayah AWS tempat Amazon Bedrock tidak tersedia, GuardDuty hasilkan jenis temuan ini hanya dari pemanggilan model Amazon SageMaker AI. Untuk Wilayah di mana Amazon Bedrock tersedia, lihat Amazon Bedrock didukung Wilayah AWS di Panduan Pengguna Amazon Bedrock.

Jenis Impact:IAMUser/PromptInjection.Direct temuan tergantung pada Amazon Bedrock Guardrails, yang tidak tersedia di semua. Wilayah AWS Jenis temuan ini hanya didukung di Wilayah di mana Amazon Bedrock Guardrails tersedia. Untuk daftar saat ini, lihat Wilayah yang Didukung untuk Pagar Batuan Dasar Amazon di Panduan Pengguna Amazon Bedrock.

Dukungan API umum

API berikut dalam Referensi Amazon GuardDuty API mungkin memiliki perbedaan regional karena tidak tersedianya beberapa sumber data atau fitur yang ditentukan Wilayah AWS sebelumnya:

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- GetDetector

- GetMemberDetectors
- DescribeOrganizationConfiguration

Jenis penemuan Amazon EC2 — dan DefenseEvasion:EC2/UnusualDoHActivity DefenseEvasion:EC2/UnusualDoTActivity

Tabel berikut menunjukkan di Wilayah AWS mana GuardDuty tersedia tetapi kedua jenis temuan Amazon EC2 ini belum didukung.

Wilayah AWS	Kode Wilayah
Asia Pasifik (Seoul)	ap-northeast-2
Asia Pacific (Osaka)	ap-northeast-3
Asia Pasifik (Jakarta)	ap-southeast-3

AWS GovCloud (US) Daerah

Untuk informasi terbaru, lihat Amazon GuardDuty di Panduan AWS GovCloud (US) Pengguna.

Wilayah Tiongkok

Untuk informasi terbaru, lihat Ketersediaan fitur dan perbedaan implementasi.

GuardDuty tindakan dan parameter warisan

Amazon GuardDuty telah menghentikan beberapa tindakan dan parameter API tetapi masih mendukungnya. Praktik terbaik adalah menggunakan tindakan dan parameter API baru yang menggantikan opsi lama. Tabel berikut membandingkan tindakan dan parameter lama dan baru.

Warisan actions/parameters	Baru actions/parameters	Perbandingan
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Dengan implementasi yang sama di kedua tindakan, GuardDuty gunakan istilah `Administrator` dalam`DisassociateFromAdministratorAccount` .
`autoEnable` parameter dalam DescribeOrganizationConfigurationdan UpdateOrganizationConfiguration	`autoEnableOrganizationMembers`	Dengan`autoEnableOrganizationMembers` , akun GuardDuty administrator dapat mengaudit dan menegakkan GuardDuty semua akun anggota ke salah satu nilai. Menggunakan API, mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota. Untuk informasi selengkapnya tentang kemungkinan nilai `autoEnableOrganizationMembers` bidang, lihat auto EnableOrganizationMembers
`dataSources` parameter dalam API yang tercantum dalamGuardDuty Perubahan API	`features`	Mulai Maret 2023, Anda dapat mengonfigurasi GuardDuty Perlindungan Malware untuk EC2 dan menggunakan `features` paket GuardDuty perlindungan baru. Rencana perlindungan yang diluncurkan sebelum Maret 2023,

Warisan actions/ parameters	Baru actions/parameters	Perbandingan
pada Maret 2023.		termasuk Perlindungan Malware untuk EC2 masih mendukung penggunaan konfigurasi. `dataSources` Jika Anda menggunakan API untuk mengonfigurasi paket perlindungan, setiap permintaan API dapat menyertakan `dataSources` atau`features`, tidak keduanya.

Riwayat dokumen untuk Amazon GuardDuty

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir Panduan GuardDuty Pengguna Amazon. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Fitur baru - Aturan Deteksi Kustom untuk Pemantauan Runtime	Aturan Deteksi Kustom GuardDuty sekarang mendukung Runtime Monitoring untuk mendeteksi aktivitas host dan container seperti eskalasi hak istimewa, pencurian kredenal, gangguan pertahanan, dan pelarian kontainer di Amazon EKS, Amazon EC2, dan Amazon ECS di Fargate. Untuk informasi selengkapnya, lihat Aturan Deteksi Kustom untuk Pemantauan Waktu Proses. Aturan ini juga menghasilkan empat jenis pencarian Runtime Monitoring baru. Untuk informasi selengkapnya, lihat Menemukan jenis yang memerlukan Aturan Deteksi Kustom dalam GuardDuty jenis pencarian Pemantauan Waktu Proses.	Oktober 15, 2026
Jenis temuan yang diperbarui - UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS	ResourceCredentialExfiltration.InsideAWSTemuan yang ada sekarang mendeteksi eksfiltrasi kredenal Lambda	September 28, 2026

	selain Amazon ECS. Untuk informasi selengkapnya, lihat UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS.	
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.17.1 untuk Amazon EKS, Amazon EC2, dan sumber daya Amazon ECS-.AWS Fargate Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	September 18, 2026
Dokumentasi yang diperbarui - Platform yang didukung Runtime Monitoring	GuardDuty Runtime Monitoring menambahkan halaman arsitektur CPU, sistem operasi, dan versi kernel yang didukung terkonsolidasi. Halaman prasyarat untuk instans Amazon EC2, AWS Fargate (hanya Amazon ECS), dan kluster Amazon EKS sekarang mereferensikan halaman ini untuk arsitektur CPU terverifikasi, distribusi OS, dan versi kernel. Halaman ini sekarang menyertakan kernel Bottlerocket versi 6.18.	September 18, 2026

Bidang AWS CloudTrail acara yang diedit yang didokumentasikan untuk Aturan Deteksi Kustom	Panduan tambahan yang menjelaskan bahwa AWS layanan dapat menyuntingan nilai bidang dalam AWS CloudTrail peristiwa yang diterbitkannya, dan bahwa Aturan Deteksi Kustom yang logika pendeteksiannya bergantung pada bidang yang disunting tidak cocok. Untuk informasi selengkapnya, lihat Bidang acara yang disunting.	September 18, 2026
AI Protection berkontribusi pada deteksi urutan serangan	GuardDuty Extended Threat Detection sekarang mencakup temuan Perlindungan GuardDuty AI di antara sinyal yang berkorelasi untuk mendeteksi urutan serangan. Untuk informasi selengkapnya, lihat GuardDuty Extended Threat Detection dan GuardDuty AI Protection.	September 17, 2026

GuardDuty Peran terkait layanan (SLR) yang diperbarui	GuardDuty telah memperbarui peran terkait layanan (SLR) untuk menyertakan dan izin. `vpc-lattice:CreateServiceNetworkVpcAssociation` `vpc-lattice:AssociateViaAWSService` Izin ini memungkinkan GuardDuty untuk menggunakan tindakan Amazon VPC Lattice untuk mengaktifkan konektivitas bagi agen Runtime Monitoring. Untuk informasi selengkapnya, lihat izin Service-linked peran untuk GuardDuty.	September 9, 2026
Fitur baru - Aturan Deteksi Kustom	GuardDuty memperkenalkan Aturan Deteksi Kustom, pustaka aturan deteksi yang dikuratori yang selaras dengan teknik aktor ancaman. Anda dapat menelusuri, mengaktifkan, dan mengelola aturan untuk mendeteksi teknik tertentu di lingkungan Anda. Untuk informasi selengkapnya, lihat Aturan Deteksi Kustom.	September 1, 2026

Fungsionalitas yang diperbarui - GuardDuty Investigasi (Pratinjau)	Menghapus batas 100 akun untuk investigasi tingkat organisasi. Investigasi organisasi sekarang menganalisis semua akun di organisasi Anda. Untuk informasi lebih lanjut, lihat GuardDutyInvestigasi.	Agustus 24, 2026
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.16.0 untuk Amazon EKS, Amazon EC2, dan sumber daya Amazon ECS-.AWS Fargate Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	Juli 17, 2026

Jenis temuan baru - UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS dan jenis temuan yang diperbarui - UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	GuardDuty memperkenalkan jenis temuan baru yang mendeteksi kapan AWS kredensil sementara yang dibuat untuk tugas Amazon ECS digunakan dari yang berbeda. Akun AWS Selain itu, ResourceCredentialExfiltration.OutsideAWS temuan yang ada sekarang mendeteksi eksfiltrasi kredenal tugas Amazon ECS selain Lambda. Untuk informasi selengkapnya, lihat UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS dan UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS.	Juli 15, 2026
Rencana perlindungan baru - Perlindungan GuardDuty AI	GuardDuty AI Protection mendeteksi ancaman terhadap beban kerja AI yang menggunakan Amazon Bedrock dan Amazon AI. SageMaker Saat Anda mengaktifkan Perlindungan AI, GuardDuty menganalisis peristiwa AWS CloudTrail data dari layanan ini untuk mendeteksi pemanggilan model anomali, serangan pengambilan biaya, dan upaya injeksi segera langsung. Untuk informasi selengkapnya, lihat Perlindungan GuardDuty AI.	Juli 13, 2026

Detail ancaman tambahan dalam skema EventBridge acara Amazon untuk Perlindungan Malware untuk S3	Perlindungan Malware untuk hasil pemindaian objek S3 EventBridge Acara Amazon sekarang memberikan detail ancaman tambahan. Bidang baru meliputi`source`,`itemDetails` ,`hash`, dan`itemPath`. Untuk informasi selengkapnya, lihat hasil pemindaian objek S3.	Juli 7, 2026

GuardDuty Investigasi (Pratinjau)	Amazon GuardDuty sekarang menawarkan AI-powered investigasi dalam pratinjau publik. Anda dapat membuat investigasi untuk menganalisis GuardDuty temuan dan akun secara otomatis dan menerima ringkasan terstruktur dalam hitungan menit dengan disposisi skor kepercayaan diri, klasifikasi teknik MITRE ATT&CK®, dan rekomenda si yang dapat ditindaklanjuti. Anda dapat memulai investiga si dari GuardDuty konsol, CLI, API, atau MCP Server. AWS Pratinjau tersedia dalam 10 Wilayah AWS: AS Timur (Virginia N.), AS Timur (Ohio), AS Barat (Oregon), Kanada (Tengah), Eropa (Frankfur t), Eropa (Irlandia), Eropa (London), Eropa (Paris), Eropa (Paris), Eropa (Stockholm), dan Asia Pasifik (Tokyo). Untuk informasi lebih lanjut, lihat GuardDutyInvestigasi.	22 Juni 2026
Amazon RDS untuk MariaDB dan MySQL	Database Insights sekarang tersedia.	Juni 11, 2026

Fungsionalitas yang diperbarui - Perlindungan Malware untuk S3	GuardDuty telah meningkatkan Perlindungan Malware untuk kuota S3 untuk jumlah maksimum file yang dapat diekstraksi dan dianalisis dari arsip, dan tingkat maksimum arsip bersarang yang dapat diekstraksi. Untuk informasi selengkapnya, lihat Kuota dalam Perlindungan Malware untuk S3.	Juni 9, 2026
Jenis penemuan Pemantauan Runtime Baru - Sensitive FileModified	GuardDuty Runtime Monitoring memperkenalkan 3 jenis temuan baru yang memberi tahu Anda saat file sistem yang sensitif terhadap keamanan pada instans atau container Amazon EC2 telah dimodifikasi, yang berpotensi memungkinkan musuh mendapatkan persistensi, meningkatkan hak istimewa, atau menghindari deteksi. Lihat informasi selengkapnya di Persistence:Runtime/SensitiveFileModified, Privilege Escalation:Runtime/SensitiveFileModified, dan DefenseEvasion:Runtime/SensitiveFileModified.	Juni 2, 2026

Fungsionalitas yang diperbarui - Menemukan kriteria filter	Bidang yang tidak didukung dihapus dari daftar kriteria filter pencarian. Untuk informasi lebih lanjut, lihat Memfilter temuan di GuardDuty.	29 Mei 2026
Pensiunan dua jenis temuan	Jenis PrivilegeEscalation:Kubernetes/PrivilegedContainerdan Persistence:Kubernetes/ContainerWithSensitiveMounttemuan telah pensiun.	29 Mei 2026
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring Menambahkan dukungan untuk Kubernetes versi 1.36. Untuk informasi selengkapnya, lihat Prasyarat untuk Pemantauan Runtime.	28 Mei 2026
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.15.0 untuk sumber daya Amazon ECS-.AWS Fargate Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	28 Mei 2026

Fungsionalitas yang diperbarui - Deteksi Ancaman Diperpanjang	GuardDuty Extended Threat Detection menambahkan lima tipe indikator baru ke detail pencarian urutan serangan: MALICIOUS_PACKAGE, MISCONFIGURATION, REACHABILITY, SENSITIVE_DATA, dan VULNERABILITY. Untuk informasi selengkapnya, lihat Detail pencarian urutan serangan.	20 Mei 2026
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.15.0 untuk sumber daya Amazon EKS dan Amazon EC2. Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	14 Mei 2026
Diperbarui AmazonGuardDutyServiceRolePolicy	Menambahkan `s3:ListBucket` `ecs:DescribeTasks` ,, dan `ecs:DescribeTaskDefinition` izin ke peran GuardDuty terkait layanan. Untuk informasi selengkapnya, lihat GuardDuty pembaruan kebijakan AWS terkelola.	April 23, 2026

Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.12.2 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	April 22, 2026
Fungsionalitas yang diperbarui - Bidang yang dapat disaring yang diperluas	GuardDuty sekarang mendukung pemfilteran pada bidang temuan apa pun saat membuat atau memperbarui aturan penekanan. Bidang stempel waktu menerima nilai dalam format milidetik Unix Epoch. Untuk informasi lebih lanjut, lihat Memfilter temuan di GuardDuty.	April 20, 2026
Fungsionalitas yang diperbarui - Perlindungan Malware untuk S3	EventBridge Pemberitahuan untuk hasil pemindaian objek S3 sekarang menyertakan `statusReasons` bidang `scanResultDetails` saat pemindaian dilewati. Bidang ini memberikan alasan spesifik mengapa pemindaian dilewati. Untuk informasi selengkapnya, lihat status pemindaian potensial objek S3 dan status hasil.	April 10, 2026

Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.9.2 untuk sumber daya Amazon EC2. Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	April 3, 2026
Diperbarui AmazonGuardDutyServiceRolePolicy	Menambahkan `cloudtrail:CreateServiceLinkedChannel` izin untuk mengaktifkan mekanisme tambahan untuk mengkonsumsi AWS CloudTrail acara. Untuk informasi selengkapnya, lihat GuardDuty pembaruan kebijakan AWS terkelola.	Maret 25, 2026
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring Menambahkan dukungan untuk Kubernetes versi 1.35. Untuk informasi selengkapnya, lihat Prasyarat untuk Pemantauan Runtime.	Maret 20, 2026

Kebijakan akses penuh tercakup bawah baru menggantikan. `AmazonGuardDutyFullAccess_v2` `AmazonGuardDutyFullAccess`	Efektif 13 Maret 2026, GuardDuty telah menghentikan kebijakan tersebut dan menggantinya dengan `AmazonGuardDutyFullAccess` kebijakan cakupan bawah bernama. `AmazonGuardDutyFullAccess_v2` Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AmazonGuardDutyFullAccess_v2.	Maret 13, 2026
Jenis temuan baru - CredentialAccess:IAMUser/CompromisedCredentials	GuardDuty Memperkenalkan tipe temuan baru yang mendeteksi ketika kunci akses IAM yang diamati berpotensi dikompromikan digunakan untuk menjalankan operasi API di. AWS Untuk informasi selengkapnya, lihat CredentialAccess:IAMUser/CompromisedCredentials.	Maret 6, 2026

Jenis temuan baru - UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	GuardDuty memperkenalkan tipe temuan baru yang mendeteksi saat host di luar AWS upaya menjalankan operasi AWS API menggunakan AWS kredenal sementara yang dibuat pada AWS Lambda sumber daya di lingkungan Anda. AWS Untuk informasi selengkapnya, lihat UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS.	Desember 16, 2025
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.9.1 untuk sumber daya Amazon EC2. Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	Desember 2, 2025

Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.12.1 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	Desember 2, 2025
Fungsionalitas yang diperbarui - Deteksi Ancaman Diperpanjang	GuardDuty Extended Threat Detection memperkenalkan dua tipe pencarian urutan serangan baru, AttackSequence:EC2/CompromisedInstanceGroupdan AttackSequence:ECS/CompromisedCluster, yang membantu mendeteksi serangan multi-tahap yang melibatkan instans Amazon EC2 yang dikompromikan dan cluster Amazon ECS. Aktifkan Runtime Monitoring untuk memaksimalkan deteksi ancaman. Untuk informasi selengkapnya, lihat Jenis pencarian urutan serangan.	Desember 2, 2025

Fitur baru - Wildcard dalam Aturan Penindasan	GuardDuty telah meningkatkan kemampuan penindasannya dengan diperkenalkannya Pertandingan dan NotMatches Kondisi yang mendukung wildcard. Pelanggan sekarang dapat menggunakan* (untuk mencocokkan sejumlah karakter) dan? (untuk mencocokkan paling banyak 1 karakter) sebagai wildcard saat membuat aturan penekanan. Aturan penindasan.	Desember 2, 2025
Fitur baru - Dukungan Metrik CloudWatch Penggunaan Amazon	GuardDuty memperkenalkan metrik penggunaan penerbitan di Amazon CloudWatch untuk semua paket perlindungan, memungkinkan pelanggan memantau penggunaan. Untuk informasi selengkapnya, lihat Memantau GuardDuty Penggunaan dan Memperkirakan Biaya	November 25, 2025

Jenis temuan baru - DefenseEvasion:IAMUser/BedrockLoggingDisabled	GuardDuty memperkenalkan tipe temuan baru yang mendeteksi saat pencatatan pemanggilan model Amazon Bedrock dinonaktifkan, yang mungkin mengindikasikan upaya untuk menghindari deteksi aktivitas beban kerja AI. Untuk informasi selengkapnya, lihat DefenseEvasion:IAMUser/BedrockLoggingDisabled.	November 21, 2025
Fitur baru - Perlindungan Malware untuk Backup	GuardDuty Perlindungan Malware untuk Cadangan sekarang tersedia di semua Wilayah komersial GuardDuty jika tersedia. Fitur ini membantu Anda mendeteksi potensi keberadaan malware di sumber daya cadangan Anda melalui pemindaian penuh dan bertahap dari snapshot Amazon EBS, AMI EC2, dan Poin Pemulihan. Untuk informasi selengkapnya tentang fitur ini, lihat Perlindungan Malware untuk Cadangan	November 19, 2025
Ubah ke AmazonGuardDutyFullAccess dan AmazonGuardDutyFullAccess_V2	Izin tambahan yang memungkinkan Anda meneruskan peran IAM GuardDuty saat Anda mengaktifkan Perlindungan Malware untuk Pencadangan.	November 19, 2025

Fitur baru - Perlindungan Malware untuk pemindaian sesuai permintaan S3.	GuardDuty mengumumkan Scan on Demand for Malware Protection untuk S3. Dengan menggunakan fitur ini, Anda dapat menggunakan SendObjectMalwareScan API baru untuk memicu pemindaian pada objek yang sudah ada yang disimpan di bucket S3 Anda. Untuk selengkapnya, lihat pemindaian malware S3 sesuai permintaan.	November 17, 2025
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.9.0 untuk sumber daya Amazon ECS-.AWS Fargate Untuk informasi tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	Oktober 28, 2025
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.9.0 untuk sumber daya Amazon EC2. Untuk informasi tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	Oktober 23, 2025

Jenis temuan Pemantauan Runtime Baru - DefenseEvasion:Runtime/KernelModuleLoaded	GuardDuty Runtime Monitoring memperkenalkan jenis temuan baru yang membantu Anda mengidentifikasi teknik penghindaran pertahanan di mana pelaku ancaman menggunakan modul kernel untuk melewati kontrol keamanan, memodifikasi operasi sistem, dan mendapatkan akses sistem yang persisten. Untuk informasi selengkapnya, lihat DefenseEvasion:Runtime/KernelModuleLoaded.	Oktober 15, 2025
Fungsionalitas yang diperbarui - Runtime Monitoring	Menambahkan dukungan untuk Kubernetes versi 1.34 untuk distribusi OS dan versi agen keamanan untuk Role GuardDuty SageMaker Manager untuk sumber daya Amazon EKS. Untuk informasi selengkapnya, lihat Memvalidasi persyaratan arsitektur untuk Amazon EKS.	Oktober 3, 2025

Menambahkan panduan pemecahan masalah untuk masalah database Amazon RDS	Menambahkan panduan untuk menyelesaikan masalah database RDS yang dapat memengaruhi kemampuan pemantauan Perlindungan GuardDuty RDS, termasuk `storage-full` status dan RDS untuk persyaratan replika baca PostgreSQL. Untuk informasi selengkapnya, lihat Memecahkan masalah pemantauan Perlindungan RDS.	September 15, 2025
Fungsionalitas yang diperbarui - Runtime Monitoring	Menambahkan distribusi Ubuntu Noble OS dengan dukungan untuk kernel versi 6.13 dan 6.14 untuk GuardDuty Runtime Monitoring untuk Amazon EC2. Untuk informasi tentang versi agen EC2 yang didukung untuk distribusi OS ini, lihat Memvalidasi persyaratan arsitektur untuk Amazon EC2.	September 13, 2025
Fungsionalitas yang diperbarui - Perlindungan RDS	Ditambahkan PostgreSQL 17 dukungan untuk RDS untuk database PostgreSQL dipantau oleh RDS Protection. GuardDuty Untuk informasi selengkapnya, lihat Database yang didukung di Perlindungan RDS.	September 13, 2025

Fungsionalitas yang diperbarui - Perlindungan Malware untuk S3	GuardDuty Perlindungan Malware untuk S3 meningkatkan kuota default file arsip yang diekstrak dari 1.000 menjadi 10.000 file. Untuk informasi selengkapnya, lihat Kuota dalam Perlindungan Malware untuk S3.	September 3, 2025
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.11 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	Agustus 29, 2025
Fungsionalitas yang diperbarui - Bekerja dengan daftar	GuardDuty memperkenalkan daftar entitas terpercaya dan ancaman khusus yang mendukung alamat IP dan nama domain. GuardDuty terus mendukung daftar alamat IP dan merekomendasikan penggunaan daftar entitas untuk deteksi ancaman khusus. Untuk informasi selengkapnya, lihat Menyesuaikan deteksi ancaman dengan daftar entitas dan daftar alamat IP.	Agustus 15, 2025

Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.8.0 untuk sumber daya Amazon EC2 dan Amazon ECS-.AWS Fargate Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	Agustus 12, 2025
Support untuk Wilayah Asia Pasifik (Taipei)	Amazon sekarang GuardDuty tersedia di Wilayah Asia Pasifik (Taipei) (`ap-east-2`). Untuk mengaktifkan GuardDuty di Wilayah ini, lihat Memulai. Anda dapat menerima pemberitahuan tentang pembaruan GuardDuty fitur dan deteksi ancaman dengan Berlangganan pengumuman Amazon GuardDuty SNS di Wilayah ini.	Juli 31, 2025
Fungsionalitas yang diperbarui - Perlindungan Malware untuk S3	Perlindungan Malware untuk S3 sekarang mendukung pemindaian objek hingga 100 GB, meningkat dari 5 GB. Ini termasuk objek individual dan file arsip yang diekstraksi. Untuk informasi selengkapnya, lihat Perlindungan Malware untuk kuota S3.	Juli 23, 2025

Fungsionalitas yang diperbarui - Menambahkan pemilik bucket yang diharapkan dalam IP kepercayaan dan daftar ancaman	GuardDuty menambahkan bidang Expected bucket owner untuk IP tepercaya dan daftar IP ancaman. Di bidang opsional ini, Anda dapat menentukan Akun AWS ID yang GuardDuty akan digunakan untuk memverifikasi kepemilikan bucket Amazon S3. Untuk informasi lebih lanjut, lihat Menggunakan daftar IP tepercaya dan daftar ancaman.	Juli 16, 2025
Fungsionalitas yang diperbarui - Deteksi Ancaman Diperpanjang	GuardDuty Extended Threat Detection kini memperluas dukungan untuk klaster Amazon EKS dengan menghubungkan beberapa sinyal keamanan di seluruh log audit EKS, perilaku proses runtime, dan aktivitas API. AWS Aktifkan Perlindungan EKS, Runtime Monitoring (dengan add-on EKS), atau keduanya untuk memaksimalkan deteksi ancaman. Untuk mengidentifikasi potensi ancaman, GuardDuty perkenalkan jenis temuan baru — AttackSequence:EKS/CompromisedCluster. Untuk informasi selengkapnya, lihat Deteksi Ancaman Diperpanjang.	Juni 17, 2025

Fungsionalitas yang diperbarui - Perlindungan Malware untuk S3	Perlindungan Malware untuk S3 tidak mendukung pemindaian arsip dengan rasio kompresi yang sangat tinggi. File-file ini akan dilewati selama pemindaian dan ditandai dengan hasil pemindaian. `UNSUPPORTED` Untuk informasi selengkapnya, lihat status pemindaian potensial objek S3 dan status hasil.	Juni 13, 2025
Fungsionalitas yang diperbarui - Perlindungan Malware untuk EC2	Perlindungan Malware untuk EC2 telah menambahkan dukungan untuk memindai sebagian besar instance dengan `productCode` as. `marketplace` Ini berlaku untuk pemindaian GuardDuty-initiated malware dan pemindaian On-demand malware. Untuk informasi selengkapnya, lihat Alasan melewatkan sumber daya selama pemindaian malware.	Juni 13, 2025

Kebijakan AmazonGuardDutyFullAccess _v2 baru	Menambahkan AmazonGuardDutyFullAccess_v2 kebijakan baru dengan izin untuk meningkatkan keamanan dengan membatasi tindakan administratif pada prinsipal GuardDuty layanan. Untuk informasi tentang kebijakan yang direkomendasikan ini, lihat kebijakan AWS terkelola: AmazonGuardDutyFullAccess_v2.	4 Juni 2025
Dukungan Wilayah yang Diperluas untuk Perlindungan RDS	GuardDuty Perlindungan RDS sekarang tersedia di Wilayah Meksiko (Tengah), Asia Pasifik (Thailand), dan Asia Pasifik (Malaysia). Perlindungan RDS membantu Anda mendeteksi perilaku login yang berpotensi mencurigakan di Aurora MySQL yang didukung, Aurora PostgreSQL (termasuk Limitless Database), dan RDS untuk PostgreSQL. Dalam hal deteksi ancaman, GuardDuty menghasilkan temuan Perlindungan RDS. Untuk informasi selengkapnya tentang basis data yang didukung dan mengaktifkan rencana perlindungan ini di Wilayah yang baru didukung, lihat Perlindungan RDS.	4 Juni 2025

Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.7.1 untuk sumber daya Amazon EC2. Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	3 Juni 2025
Support untuk Extended Threat Detection	GuardDuty Extended Threat Detection sekarang tersedia di Asia Pasifik (Thailand) (ap-tenggara - 7). Tanpa aktivasi yang diperlukan, ia mendeteksi serangan multi-tahap yang menjangkau sumber data, berbagai jenis sumber AWS daya, dan waktu, dalam file. Akun AWS Ketika ancaman potensial terdeteksi, itu menghasilkan temuan urutan serangan. Untuk informasi selengkapnya, lihat Deteksi Ancaman Diperpanjang.	12 Mei 2025

Support untuk Wilayah Meksiko (Tengah)	Amazon sekarang GuardDuty tersedia di Wilayah Meksiko (Tengah) `mx-central-1` (). Untuk mengaktifkan GuardDuty di Wilayah ini, lihat Memulai. Anda dapat menerima pemberitahuan tentang pembaruan GuardDuty fitur dan deteksi ancaman dengan Berlangganan pengumuman Amazon GuardDuty SNS di Wilayah ini.	7 Mei 2025
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.10.0 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	April 4, 2025
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.7.0 untuk sumber daya Amazon. ECS-Fargate Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	April 4, 2025

Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.7.0 untuk sumber daya Amazon EC2. Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	April 3, 2025
Support untuk Wilayah Asia Pasifik (Thailand)	Amazon sekarang GuardDuty tersedia di Wilayah Asia Pasifik (Thailand). Untuk informasi tentang fitur yang didukung di Wilayah ini, lihat ketersediaan Region-specific fitur. Untuk mengaktifkan GuardDuty di Wilayah ini, lihat Memulai. Anda dapat menerima pemberitahuan tentang pembaruan GuardDuty fitur dan deteksi ancaman dengan Berlangganan pengumuman Amazon GuardDuty SNS.	April 1, 2025

Fungsionalitas diperbarui	Dasbor Ringkasan sekarang menunjukkan wawasan berdasarkan semua temuan keamanan yang dihasilkan, menghilangkan batasan 5.000 temuan sebelumnya. Untuk informasi tentang wawasan ini, lihat Dasbor GuardDuty ringkasan.	Maret 17, 2025
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.9.0 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	Maret 2, 2025
Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring telah menambahkan jenis masalah cakupan baru (Agen Tidak Disediakan) untuk sumber daya Amazon EC2. Untuk informasi tentang pemecahan masalah ini, lihat Memecahkan masalah cakupan waktu proses Amazon EC2.	Februari 21, 2025

Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring merilis agen keamanan baru untuk Amazon EC2 dan sumber daya Amazon ECS-Fargate . Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat versi rilis agen GuardDuty keamanan.	Februari 6, 2025
GuardDuty dukungan di Wilayah Asia Pasifik (Malaysia) yang ada	GuardDuty Extended Threat Detection sekarang tersedia di Wilayah Asia Pasifik (Malaysia). Untuk informasi selengkapnya, lihat Deteksi Ancaman Diperpanjang.	Januari 28, 2025
Support untuk Wilayah Asia Pasifik (Malaysia)	Amazon sekarang GuardDuty tersedia di Wilayah Asia Pasifik (Malaysia). Untuk informasi tentang fitur yang didukung di Wilayah ini, lihat ketersediaan Region-specific fitur. Untuk mengaktifkan GuardDuty di Wilayah ini, lihat Memulai. Anda dapat menerima pemberitahuan tentang pembaruan GuardDuty fitur dan deteksi ancaman dengan Berlangganan pengumuman Amazon GuardDuty SNS.	Januari 16, 2025

Fungsionalitas yang diperbarui - Runtime Monitoring	GuardDuty Runtime Monitoring telah memperbarui informasi tambahan dan langkah-langkah pemecahan masalah untuk masalah ECS-Fargate cakupan Amazon yang terkait dengan Agen yang tidak disediakan. Untuk informasi selengkapnya tentang Agen bukan jenis masalah yang disediakan, lihat Memecahkan masalah cakupan waktu proses ECS-Fargate Amazon.	Januari 8, 2025
Jenis temuan baru - Policy:IAMUser/ShortTermRootCredentialUsage	GuardDuty memperkenalkan jenis temuan baru yang memberi tahu Anda saat kredensi pengguna terbatas, yang dibuat untuk yang tercantum Akun AWS di lingkungan Anda, digunakan untuk membuat permintaan. Layanan AWS Untuk informasi selengkapnya, lihat Policy:IAMUser/ShortTermRootCredentialUsage.	Januari 8, 2025

Fitur baru - Deteksi Ancaman GuardDuty Diperpanjang	GuardDuty mengumumkan Extended Threat Detection untuk mendeteksi urutan serangan multi-tahap yang menjangkau sumber data GuardDuty dasar dan sumber AWS daya di Anda Akun AWS, selama periode waktu tertentu. Tanpa biaya tambahan, kemampuan ini diaktifkan secara otomatis untuk semua akun yang telah diaktifkan GuardDuty. Fitur ini mengumumkan dua jenis GuardDuty temuan baru, yang disebut Attack sequence finding types. Untuk informasi selengkapnya, lihat Deteksi Ancaman Diperpanjang.	Desember 1, 2024

Fungsionalitas lintas layanan yang ditingkatkan - Pemantauan Runtime dan Perlindungan Malware untuk EC2	Dampak fitur Amazon Elastic Kubernetes Service (Amazon EKS) baru pada fitur Amazon: GuardDuty • Mode Otomatis Amazon EKS - Pemantauan Runtime untuk Amazon EKS dan Perlindungan Malware untuk EC2 mendukung ini. • Amazon EKS Hybrid Nodes — Baik Runtime Monitoring untuk Amazon EKS dan Perlindungan Malware untuk EC2 tidak mendukung ini. Untuk informasi selengkapnya, lihat Cara Runtime Monitoring bekerja dengan klaster Amazon EKS dan Perlindungan Malware untuk EC2.	Desember 1, 2024

Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon EKS	Runtime Monitoring merilis agen baru versi 1.8.1 (v1.8.1-eks-build.2) untuk sumber daya Amazon EKS. Dengan versi agen baru ini, GuardDuty memperluas dukungan Runtime Monitoring untuk sumber daya Amazon EKS yang berjalan di, RedHat CentOS, dan Fedora. Untuk informasi selengkapnya, lihat Memvalidasi persyaratan arsitektur. Untuk informasi tentang catatan rilis, lihat agen GuardDuty keamanan untuk sumber daya Amazon EKS.	November 23, 2024
Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon EC2	Runtime Monitoring merilis agen baru versi 1.5.0 untuk sumber daya Amazon EC2. Dengan versi agen baru ini, GuardDuty memperluas dukungan Runtime Monitoring untuk sumber daya Amazon EC2 yang berjalan di RedHat, CentOS, dan Fedora. Untuk informasi selengkapnya, lihat Memvalidasi persyaratan arsitektur. Untuk informasi tentang catatan rilis, lihat agen GuardDuty keamanan untuk sumber daya Amazon EC2.	November 20, 2024

Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon ECS-Fargate	Runtime Monitoring merilis agen baru versi 1.5.0 untuk sumber daya Amazon ECS-Fargate . Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk AWS Fargate (khusus Amazon ECS).	November 14, 2024
Fungsionalitas yang diperbarui dalam Perlindungan Malware untuk EC2	GuardDuty Perlindungan Malware untuk EC2 telah menambahkan tiga jenis pencarian Runtime Monitoring ke daftar Temuan yang memanggil pemindaian GuardDuty-initiated malware di instans Amazon EC2. Akun yang telah mengaktifkan Perlindungan Malware untuk EC2 akan mengamati pemindaian GuardDuty-initiated malware saat GuardDuty menghasilkan salah satu temuan berikut: • Execution:Runtime/MaliciousFileExecuted • Execution:Runtime/SuspiciousShellCreated • PrivilegeEscalation:Runtime/ElevationToRoot	November 7, 2024

Fungsionalitas yang diperbarui dalam Perlindungan RDS	GuardDuty RDS Protection menambahkan versi mesin Aurora PostgreSQL Limitless Database yang baru dirilis ke daftar database yang didukung. `16.4-limitless` Untuk Akun AWS itu telah mengaktifkan Perlindun gan RDS, secara otomatis GuardDuty akan mulai memantau perilaku login untuk Limitless Database. Akun yang telah menggunakan uji coba gratis 30 hari untuk Perlindun gan RDS akan dikenakan biaya penggunaan yang terkait dengan Limitless Database, bersama dengan basis data lain yang didukung yang dipantau. Untuk informasi selengkapnya, lihat Perlindun gan RDS.	6 November 2024

Perluasan wilayah - GuardDuty dan AWS PrivateLink integrasi	GuardDuty sekarang memperluas dukungan Wilayah untuk Amazon GuardDuty dan antarmuka VPC AWS PrivateLink endpoint (). Sebelumnya, dukungan Wilayah tersedia untuk AS Timur (Virginia N.), Eropa (Irlandia), dan Israel (Tel Aviv). Dukungan ini sekarang diperluas ke semua Wilayah AWS tempat GuardDuty yang tersedia. Untuk informasi selengkapnya tentang perbedaan regional, lihat ketersediaan Region-specific fitur.	6 November 2024
Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon ECS-Fargate	Runtime Monitoring merilis agen baru versi 1.4.1 untuk sumber daya Amazon ECS-Fargate . Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk AWS Fargate (khusus Amazon ECS).	Oktober 24, 2024

Ditambahkan dukungan untuk operasi GuardDuty CloudFormation tag	GuardDuty sekarang mendukung pembaruan kunci tag dan nilai, dan tag tingkat tumpukan. Untuk melakukan ini, tambahkan `guardduty:tagResource` izin ke peran IAM. Untuk selengkapnya GuardDuty CloudFormation, lihat referensi jenis GuardDuty sumber daya Amazon di Panduan AWS CloudFormation Pengguna.	Oktober 24, 2024
Fungsionalitas yang diperbarui dalam Perlindungan GuardDuty Malware untuk S3	Saat mengaktifkan perlindungan malware untuk S3, Anda dapat memilih peran layanan yang memiliki izin yang diperlukan untuk melakukan tindakan pemindaian malware atas nama Anda. Untuk informasi selengkapnya tentang mengaktifkan Perlindungan Malware untuk S3, lihat Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket S3 Anda.	Oktober 22, 2024

Fungsionalitas diperbarui	GuardDuty menyempurnakan jenis UnauthorizedAccess :IAMUser/InstanceCredential Exfiltration.InsideAWStemuan untuk mendeteksi penggunaa n kredensional AWS instans Amazon EC2 dari AWS PrivateLink titik akhir VPC (Akun AWS) yang tidak terkait dengan peran instans Amazon EC2. GuardDuty Kemampuan baru ini mendeteksi potensi penyalahg unaan kredensi instans Amazon EC2 dan menyediak an konteks Akun AWS remote menggunakan kredenal sesi eksfiltrasi. Untuk informasi selengkapnya tentang titik akhir AWS layanan yang didukung oleh deteksi baru ini, lihat Mencatat peristiwa aktivitas jaringan di Panduan AWS CloudTrail Pengguna.	Oktober 21, 2024

Fungsionalitas yang diperbarui - GuardDuty Runtime Monitoring	GuardDuty Runtime Monitoring menambahkan tiga jenis pencarian berikut yang memberi tahu Anda saat perintah mencurigakan dijalankan pada instans Amazon EC2 atau beban kerja container dalam lingkungan Anda: AWS • Discovery:Runtime/SuspiciousCommand • Persistence:Runtime/SuspiciousCommand • PrivilegeEscalation:Runtime/SuspiciousCommand	Oktober 10, 2024
Fitur baru - Menambahkan dukungan untuk titik akhir VPC	GuardDuty sekarang terintegrasi dengan AWS PrivateLink dan mendukung titik akhir VPC. Untuk informasi selengkapnya tentang AWS PrivateLink integrasi, lihat Amazon GuardDuty dan antarmuka VPC endpoint ().AWS PrivateLink	September 17, 2024
Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon EKS	Runtime Monitoring merilis agen baru versi 1.7.1 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk Amazon EKS.	September 13, 2024

Fungsionalitas yang diperbarui dalam Perlindungan Malware untuk S3	Perlindungan Malware untuk S3 menambahkan bidang baru,`s3Throttled` , ke skema hasil pemindaian objek S3 Amazon EventBridge (EventBridge). `s3Throttled` Bidang menunjukkan apakah ada penundaan dalam mengunggah atau mengambil penyimpanan dari bucket Amazon Simple Storage Service (Amazon S3) atau tidak. Untuk informasi selengkapnya, lihat Memantau pemindaian objek S3 dengan Amazon. EventBridge	September 13, 2024
Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon EC2	Runtime Monitoring merilis agen baru versi 1.3.1 untuk sumber daya Amazon EC2. Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk Amazon EC2.	September 12, 2024
Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon ECS-Fargate	Runtime Monitoring merilis agen baru versi 1.3.1 untuk sumber daya Amazon ECS-Fargate . Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk AWS Fargate (khusus Amazon ECS).	September 11, 2024

GuardDuty Peran terkait layanan (SLR) yang diperbarui	GuardDuty telah memperbarui SLR untuk menyertakan `ec2:Describe:Vpcs` izin dalam tindakan Amazon EC2. Untuk informasi selengkapnya, lihat izin Service-linked peran untuk GuardDuty.	Agustus 22, 2024
Penambahan konten yang signifikan	GuardDuty menambahkan pembaruan konten yang signifikan ke fitur Perlindungan Malware untuk S3. • Menambahkan contoh baru skema pemberitahuan sampel untuk menyiapkan EventBridge aturan Amazon agar menerima pemberitahuan terkait status sumber daya paket Perlindungan Malware dan hasil pemindaian objek S3. Untuk informasi selengkapnya, lihat Memantau pemindaian objek S3 dengan Amazon. EventBridge • Menambahkan informasi tentang pemecahan masalah kegagalan tag pasca-pemindaian objek S3.	Agustus 20, 2024

Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Amazon EC2	Runtime Monitoring merilis agen baru versi 1.3.0 untuk sumber daya Amazon EC2. Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk Amazon EC2.	Agustus 19, 2024
Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Amazon EKS	Runtime Monitoring merilis agen baru versi 1.7.0 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk klaster Amazon EKS.	Agustus 17, 2024
Penambahan konten yang signifikan	GuardDuty menambahkan informasi baru tentang metodologi deteksi malware dan mesin pemindaian yang digunakannya untuk Perlindungan Malware untuk S3 dan Perlindungan Malware untuk fitur EC2. Untuk informasi selengkapnya, lihat mesin pemindaian deteksi GuardDuty malware.	Agustus 15, 2024

Fitur baru - Melindungi beban kerja AI	GuardDuty deteksi ancaman dasar dan Perlindungan Lambda membantu Anda mengamankan dan mendeteksi ancaman terhadap beban kerja AI yang dibangun dengan lebih baik. AWS Untuk informasi selengkapnya, lihat Melindungi beban kerja AI dengan GuardDuty.	Agustus 14, 2024
Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Fargate (hanya Amazon ECS)	Runtime Monitoring merilis agen baru versi 1.3.0 untuk sumber daya (hanya AWS Fargate Amazon ECS). Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk Fargate-ECS.	Agustus 9, 2024
Fungsionalitas yang diperbarui - Perlindungan Malware untuk S3	GuardDuty Perlindungan Malware untuk S3 meningkatkan jumlah maksimum kuota bucket S3 dari 10 menjadi 25 bucket. Kuota ini berlaku untuk Akun AWS per masing-masing Wilayah AWS. Untuk informasi selengkapnya, lihat Perlindungan Malware untuk S3.	Agustus 8, 2024

Diperbarui - Jenis temuan baru di Runtime Monitoring	GuardDuty telah menambahkan dua jenis temuan Pemantauan Runtime baru yang akan membantu Anda mendeteksi ancaman yang melibatkan pembuatan shell yang mencurigakan pada sumber daya yang dipantau, dan eskalasi hak istimewa di mana suatu proses secara mencurigakan meningkatkan hak istimewanya untuk melakukan root. • Execution:Runtime/SuspiciousShellCreated • PrivilegeEscalation:Runtime/ElevationToRoot	Agustus 6, 2024
Diperbarui - Mengintegrasikan dengan AWS Security Hub CSPM	AWS Security Hub CSPM menyediakan daftar kontrol GuardDuty keamanan untuk mengevaluasi sumber daya Anda, dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk informasi selengkapnya, lihat Menggunakan GuardDuty kontrol di CSPM Security Hub.	Juli 11, 2024

Skrip GuardDuty tester yang diperbarui untuk temuan	GuardDuty sekarang mendukung lebih dari 100 temuan dengan AWS sumber daya yang berbeda di akun khusus. Untuk informasi lebih lanjut, lihat GuardDuty Temuan uji di akun khusus.	Juni 28, 2024
Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring merilis agen keamanan baru versi 1.2.0 untuk sumber daya Amazon EC2. Untuk informasi tentang catatan rilis, lihat agen GuardDuty keamanan untuk instans Amazon EC2. Untuk informasi tentang memperbarui agen keamanan ke versi rilis ini secara manual, lihat Mengelola agen keamanan secara manual untuk instans Amazon EC2.	Juni 13, 2024

Fitur baru - Perlindungan Malware untuk ketersediaan Wilayah S3	GuardDuty Perlindungan Malware untuk S3 sekarang tersedia di semua Wilayah komersial di mana GuardDuty tersedia. Fitur ini membantu Anda memindai objek yang baru diunggah ke bucket Amazon S3 untuk mencari potensi malware dan unggahan yang mencuriga kan, dan mengambil tindakan untuk mengisolasinya sebelum dimasukkan ke dalam proses hilir. Untuk informasi tentang mengaktifkan Perlindun gan Malware untuk S3, lihat Perlindungan GuardDuty Malware untuk S3.	Juni 12, 2024

Fitur baru - Perlindungan Malware untuk S3	GuardDuty mengumumkan ketersediaan umum Perlindungan Malware untuk S3 yang membantu Anda memindai objek yang baru diunggah ke bucket Amazon S3 untuk mencari potensi malware dan unggahan yang mencurigakan, dan mengambil tindakan untuk mengisolasinya sebelum tertelan ke dalam proses hilir. Fitur ini sepenuhnya dikelola oleh AWS. GuardDuty menerbitkan hasil pemindaian objek S3 ke bus acara EventBridge default Anda. Anda dapat mengizinkan GuardDuty untuk menambahkan tag ke objek S3 yang dipindai. Anda dapat membuat alur kerja hilir, seperti isolasi ke bucket karantina, atau menentukan kebijakan bucket menggunakan tag yang mencegah pengguna atau aplikasi mengakses objek tertentu. Untuk informasi selengkapnya, lihat Perlindungan GuardDuty Malware untuk S3. Saat ini, tersedia di Wilayah berikut: • Timur AS (N. Virginia) • AS Timur (Ohio) • AS Barat (Oregon) • Europe (Ireland)	Juni 11, 2024

	• Eropa (Frankfurt) • Eropa (Stockholm) • Asia Pasifik (Sydney) • Asia Pacific (Tokyo) • Asia Pacific (Singapore) (Asia Pacific (Singapore))	
AmazonGuardDutyFullAccessKebijakan yang diperbarui	Menambahkan izin yang memungkinkan Anda meneruskan peran IAM GuardDuty saat Anda mengaktifkan Perlindungan Malware untuk S3. Untuk informasi selengkapnya tentang pembaruan kebijakan ini, lihat kebijakan AWS terkelola: AmazonGuardDutyFullAccess.	Juni 10, 2024
Fungsionalitas yang diperbarui dalam GuardDuty Perlindungan RDS	Perlindungan RDS memperluas dukungan untuk memantau aktivitas login pada RDS Anda untuk database PostgreSQL. Sebagai bagian dari ekspansi ini, secara otomatis GuardDuty akan mulai memantau data login dari RDS untuk database PostgreSQL untuk akun yang telah mengaktifkan Perlindungan RDS. GuardDuty Untuk informasi selengkapnya, lihat Perlindungan RDS.	Juni 6, 2024

Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Fargate (hanya Amazon ECS)	Runtime Monitoring merilis agen baru versi 1.2.0 untuk sumber daya (hanya AWS Fargate Amazon ECS). Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk Fargate-ECS.	31 Mei 2024
Fungsionalitas yang diperbarui dalam Perlindungan GuardDuty Malware untuk EC2	Untuk setiap volume Amazon EBS yang dilampirkan ke instans Amazon EC2 dan beban kerja kontainer GuardDuty , Perlindungan Malware untuk EC2 telah meningkatkan ukuran volume EBS yang dipindai hingga 2048 GB. Untuk informasi tentang pemindaian volume Amazon EBS yang dilampirk an ke instans Anda, lihat Perlindungan GuardDuty Malware untuk EC2.	29 Mei 2024
Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring untuk ECS-Fargate sumber daya Amazon sekarang mendukung pendeteksian potensi ancaman pada tugas yang diluncurkan oleh AWS Batch dan. AWS CodePipeline Untuk informasi selengkapnya, lihat Cara Runtime Monitorin g bekerja dengan Fargate (hanya Amazon ECS).	28 Mei 2024

Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring merilis agen baru versi 1.6.1 untuk sumber daya Amazon EKS. Untuk informasi tentang catatan rilis, lihat riwayat rilis agen add-on EKS.	14 Mei 2024
Dukungan Wilayah yang Diperluas untuk Runtime Monitoring	GuardDuty memperluas dukungan untuk Runtime Monitoring ke Wilayah Kanada Barat (Calgary) . Untuk informasi tentang memulai Runtime Monitorin g, lihat Mengaktifkan Runtime Monitoring.	7 Mei 2024
Dukungan Wilayah yang Diperluas untuk Perlindungan RDS	GuardDuty memperluas dukungan Perlindungan RDS menjadi berikut: Wilayah AWS • Kanada Barat (Calgary) • Asia Pasifik (Hyderabad) • Eropa (Spanyol) • Eropa (Zürich) • Timur Tengah (UAE) • Israel (Tel Aviv) • Asia Pacific (Melbourne) Untuk informasi tentang mengaktifkan fitur ini, lihat Perlindungan RDS.	3 Mei 2024

Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring merilis agen baru versi 1.1.0 untuk sumber daya (hanya AWS Fargate Amazon ECS). Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk Fargate-ECS.	1 Mei 2024
Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring merilis agen baru versi 1.6.0 untuk sumber daya Amazon EKS. Untuk informasi tentang catatan rilis, lihat riwayat rilis agen add-on EKS.	April 29, 2024
Support untuk IPAddressV6	GuardDuty telah menambahkan dukungan IPAddressV6 untuk detail IP lokal dan jarak jauh. Anda dapat menggunakan atribut Filter terkait untuk memfilter GuardDuty temuan atau membuat aturan penekanan.	April 18, 2024
Pengalaman konsol yang diperbarui untuk mengonfigurasi temuan ekspor	GuardDuty telah memperbarui pengalaman konsol untuk mengekspor temuan yang dihasilkan di Akun AWS ember Amazon S3 Anda. Untuk informasi lebih lanjut, lihat Mengekspor GuardDuty temuan.	April 1, 2024

Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring merilis agen keamanan baru versi 1.1.0 untuk sumber daya Amazon EC2. Versi ini mendukung konfigurasi agen GuardDuty otomatis dalam Runtime Monitoring untuk instans Amazon EC2. Untuk informasi tentang catatan rilis, lihat agen GuardDuty keamanan untuk instans Amazon EC2.	Maret 28, 2024

Ketersediaan umum Runtime Monitoring untuk instans Amazon EC2	GuardDuty mengumumkan ketersediaan umum (GA) Runtime Monitoring untuk instans Amazon EC2. Sekarang, Anda memiliki opsi untuk mengaktifkan konfigurasi agen otomatis yang memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk instans Amazon EC2 Anda atas nama Anda. Dengan agen GuardDuty otomatis, Anda juga dapat menggunakan tag penyertaan atau pengecualian untuk menginformasikan GuardDuty agar menginstal dan mengelola agen keamanan hanya pada instans Amazon EC2 tertentu. Untuk informasi selengkapnya, lihat Cara kerja Runtime Monitoring dengan instans Amazon EC2. Daftar jenis temuan baru yang dirilis bersama dengan GA ini • Execution:Runtime/SuspiciousTool • Execution:Runtime/SuspiciousCommand • DefenseEvasion:Runtime/SuspiciousCommand	Maret 28, 2024

- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted

Amazon GuardDuty telah memperbarui Service-linked peran (SLR)	Gunakan AWS Systems Manager tindakan untuk mengelola asosiasi SSM di instans Amazon EC2 saat Anda GuardDuty mengaktifkan Pemantauan Waktu Proses dengan agen otomatis untuk Amazon EC2. Ketika konfigura si agen GuardDuty otomatis dinonaktifkan, GuardDuty pertimbangkan hanya instans EC2 yang memiliki tag inklusi (`GuardDuty Managed :true`). • Daftar berikut menunjukkan izin baru: `"ssm:DescribeAssoc iation", "ssm:DeleteAssocia tion", "ssm:UpdateAssociati on", "ssm:CreateAs sociation", "ssm:StartAssoc iationsOnce", "ssm:AddTagsT oResource", "ssm:CreateAsso ciation", "ssm:UpdateAssoci ation", "ssm:SendCommand", "ssm:GetCommandInv ocation"`	26 Maret 2024

Fungsionalitas yang diperbarui di Runtime Monitoring	Dengan rilis v1.5.0 agen GuardDuty keamanan terbaru (add-on) untuk Amazon EKS, Runtime Monitoring sekarang mendukung konfigurasi parameter spesifik agen GuardDuty keamanan Anda, seperti pengaturan CPU dan memori, pengaturan, dan `PriorityClass` pengaturan kebijakan DNS. Untuk informasi selengkapnya, lihat Mengonfigurasi GuardDuty parameter agen keamanan (EKS add-on).	7 Maret 2024
Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring merilis agen baru versi 1.5.0 untuk sumber daya Amazon EKS. Untuk informasi tentang catatan rilis, lihat riwayat rilis agen add-on EKS.	7 Maret 2024
Dukungan untuk Kanada Barat (Calgary)	Amazon sekarang GuardDuty tersedia di Wilayah Kanada Barat (Calgary). Beberapa rencana perlindungan di dalamnya GuardDuty mungkin tidak tersedia di Wilayah ini. Untuk informasi terbaru, lihat Wilayah dan titik akhir.	Maret 6, 2024

Fungsionalitas yang diperbarui di Runtime Monitoring	Agen GuardDuty keamanan versi 1.0.0 dan 1.1.0 untuk kluster Amazon EKS tidak akan lagi didukung mulai 14 Mei 2024. Untuk informasi tentang langkah-langkah apa yang dapat Anda ambil sebelum akhir dukungan standar, lihat agen GuardDuty keamanan untuk klaster Amazon EKS.	Februari 16, 2024
Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring mendukung Kubernetes versi 1.29 terbaru dengan agen keamanan versi 1.4.1 yang ada. Dukungan telah tersedia sejak peluncuran versi Kubernetes ini. Untuk informasi tentang versi Kubernetes yang didukung, lihat Versi Kubernetes yang didukung oleh agen keamanan. GuardDuty	Februari 16, 2024

Fungsionalitas yang diperbarui dalam Runtime Monitoring - Ketersediaan regional	GuardDuty Runtime Monitoring sekarang mendukung VPC Amazon bersama dalam hal yang sama. AWS Organizations GuardDuty peran terkait layanan (SLR) memiliki izin baru — `organizations:DescribeOrganization` yang membantu mengambil ID organisasi untuk akun VPC Amazon bersama untuk menetapkan kebijakan titik akhir. Untuk informasi tentang prasyarat menggunakan endpoint Amazon VPC bersama di Runtime Monitoring, lihat Support for shared Amazon VPC. Kemampuan ini tersedia di semua Wilayah yang GuardDuty mendukung Runtime Monitoring.	Februari 12, 2024

Fungsionalitas yang diperbarui dalam Runtime Monitoring - Ketersediaan regional	GuardDuty Runtime Monitoring sekarang mendukung VPC Amazon bersama dalam hal yang sama. AWS Organizations GuardDuty peran terkait layanan (SLR) memiliki izin baru — `organizations:DescribeOrganization` yang membantu mengambil ID organisasi untuk akun VPC Amazon bersama untuk menetapkan kebijakan titik akhir. Untuk informasi tentang prasyarat menggunakan endpoint Amazon VPC bersama di Runtime Monitoring, lihat Support for shared Amazon VPC. Saat ini, kemampuan ini tersedia di beberapa. Wilayah AWS Untuk informasi selengkapnya, lihat Wilayah dan titik akhir.	Februari 9, 2024
Fungsionalitas yang diperbarui dengan dukungan untuk yang baru Wilayah AWS - Perlindungan Malware untuk EC2	Perlindungan Malware untuk EC2 sekarang mendukung pemindaian volume EBS yang dienkripsi Kunci yang dikelola AWS di Wilayah AS Barat (Oregon).	Februari 6, 2024

Fungsionalitas yang diperbarui dengan dukungan untuk yang baru Wilayah AWS - Perlindungan Malware untuk EC2	Perlindungan Malware untuk EC2 sekarang mendukung pemindaian volume EBS yang dienkripsi dengan Kunci yang dikelola AWS berikut ini: Wilayah AWS • Asia Pacific (Singapore) (`ap-southeast-1`) • Europe (Frankfurt) (`eu-central-1`) • Asia Pacific (Osaka) (`ap-northeast-3`) • US East (Ohio) (`us-east-2`) • Europe (Milan) (`eu-south-1`) • Asia Pacific (Tokyo) (`ap-northeast-1`) • Asia Pacific (Seoul) (`ap-northeast-2`) • Canada (Central) (`ca-central-1`) • Europe (Ireland) (`eu-west-1`) • US East (N. Virginia) (`us-east-1`)	Februari 5, 2024

Fungsionalitas yang diperbarui di Runtime Monitoring	GuardDuty Runtime Monitoring telah merilis versi agen GuardDuty keamanan baru (v1.0.2) untuk instans Amazon EC2. Versi agen ini mencakup dukungan untuk AMI Amazon ECS terbaru. Untuk informasi selengkapnya tentang riwayat rilis agen, lihat agen GuardDuty keamanan untuk instans Amazon EC2.	Februari 2, 2024

Fungsionalitas yang diperbarui dengan dukungan untuk yang baru Wilayah AWS - Perlindungan Malware untuk EC2	Perlindungan Malware untuk EC2 sekarang mendukung pemindaian volume Amazon EBS yang dienkripsi sebagai berikut: Kunci yang dikelola AWSWilayah AWS • Europe (London) (`eu-west-2`) • Europe (Stockholm) (`eu-north-1`) • Asia Pacific (Hong Kong) (`ap-east-1`) • Africa (Cape Town) (`af-south-1`) • Middle East (Bahrain) (`me-south-1`) • Asia Pasifik (Hyderabad) () `ap-south-2` • Eropa (Spanyol) `eu-south-2` () • Asia Pasifik (Melbourne) (`ap-southeast-4`) • Asia Pacific (Sydney) (`ap-southeast-2`) • Israel (Tel Aviv) (`il-central-1`)	Januari 31, 2024

Mengelola akun yang diperbarui dengan AWS Organizations	Menata ulang konten di bawah Mengelola akun dengan AWS Organizations. , menambahkan langkah-l angkah untuk mengubah akun GuardDuty administrator yang didelegasikan, dan diperbaru i Memahami hubungan antara akun GuardDuty administrator dan akun anggota.	Januari 30, 2024
Fungsionalitas yang diperbaru i dengan dukungan untuk yang baru Wilayah AWS	Perlindungan Malware untuk EC2 sekarang mendukung pemindaian volume EBS yang dienkripsi dengan Kunci yang dikelola AWS berikut ini: Wilayah AWS • Asia Pasifik (Jakarta) (`ap-southeast-3`) • US West (N. California) (`us-west-1`) • Timur Tengah (UEA) (`me-central-1`) • Eropa (Zurich) () `eu-central-2` • Asia Pacific (Mumbai) (`ap-south-1`) • South America (São Paulo) (`sa-east-1`)	Januari 29, 2024

Fungsionalitas yang diperbarui dalam Perlindungan Malware untuk EC2	Perlindungan Malware untuk EC2 sekarang mendukung pemindaian volume EBS yang dienkripsi menggunakan. Kunci yang dikelola AWSPerlindungan Malware untuk peran terkait layanan EC2 (SLR) memiliki dua izin baru — dan. `GetSnapshotBlock` `ListSnapshotBlocks` Izin ini akan membantu GuardDuty mengambil snapshot volume EBS (dienkripsi menggunakan Kunci yang dikelola AWS) dari Anda Akun AWS dan menyalinnya ke akun GuardDuty layanan sebelum memulai pemindaian malware. Saat ini, fungsi ini hanya tersedia di Eropa (Paris) (`eu-west-3`). Untuk informasi selengkapnya, lihat Volume yang didukung untuk pemindaian malware.	Januari 25, 2024
Fungsionalitas yang diperbarui di Runtime Monitoring	GuardDuty Runtime Monitoring telah merilis versi agen GuardDuty keamanan baru (v1.0.1) dengan penyetelan dan peningkatan kinerja umum. Untuk informasi selengkapnya tentang riwayat rilis agen, lihat agen GuardDuty keamanan untuk instans Amazon EC2.	23 Januari 2024

Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring merilis agen baru versi 1.4.1 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya, lihat riwayat rilis agen add-on EKS.	Januari 16, 2024
Runtime Monitoring merilis agen baru v1.4.0 untuk sumber daya Amazon EKS	Runtime Monitoring merilis agen baru versi 1.4.0 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya, lihat riwayat rilis agen add-on EKS.	21 Desember 2023

Menambahkan jenis temuan berbasis S3 dan pembelajaran AWS CloudTrail mesin (ML) ke Eropa (Zurich), Eropa (Spanyol), Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), dan Israel (Tel Aviv)	S3 berikut dan CloudTrail temuan yang mengidentifikasi perilaku anomali menggunakan model pembelajaran mesin deteksi anomali (ML) sekarang tersedia di Wilayah Eropa (Zurich), Eropa (Spanyol), Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), dan Israel (Tel Aviv): GuardDuty • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior	21 Desember 2023

	• PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty mendukung 50.000 akun anggota melalui AWS Organizations	GuardDuty Administrator yang didelegasikan sekarang dapat mengelola maksimal 50.000 akun anggota melalui AWS Organizations. Ini juga termasuk maksimal 5000 akun anggota yang terkait dengan akun GuardDuty administrator melalui undangan.	20 Desember 2023
GuardDuty Dukungan Runtime Monitoring diperluas menjadi 19 Wilayah AWS	Runtime Monitoring sekarang tersedia di Asia Pasifik (Jakarta), Eropa (Paris), Asia Pasifik (Osaka), Asia Pasifik (Seoul), Timur Tengah (Bahrain), Eropa (Spanyol), Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), Israel (Tel Aviv), AS Barat (Californ ia N.), Eropa (London), Asia Pasifik (Hong Kong), Eropa (Milan), Timur Tengah (UEA), Amerika Selatan (São Paulo), Asia Pasifik (Mumbai), Kanada (Tengah), Afrika (Cape Town), Eropa (Zurich).	6 Desember 2023

GuardDuty memperluas kemampuan Runtime Monitoring	Selain mendeteksi ancaman terhadap kluster Amazon EKS Anda, GuardDuty mengumumkan ketersediaan umum Runtime Monitoring untuk mendeteksi ancaman terhadap beban kerja Amazon ECS Anda dan rilis pratinjau untuk mendeteksi ancaman terhadap instans Amazon EC2 Anda. Untuk informasi selengkapnya tentang yang Wilayah AWS saat ini mendukung Runtime Monitoring, lihat Wilayah dan titik akhir.	26 November 2023

Amazon GuardDuty telah memperbarui Service-linked peran (SLR)	GuardDuty telah menambahkan izin baru untuk menggunakan tindakan Amazon ECS untuk mengelola dan mengambil informasi tentang kluster Amazon ECS, dan mengelola pengaturan akun Amazon ECS. `guardduty Activate` Tindakan yang berkaitan dengan Amazon ECS juga mengambil informasi tentang tag yang terkait dengannya. GuardDuty • Izin berikut telah ditambahkan sebagai bagian dari GuardDuty perluasan kemampuan Runtime Monitoring: `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	26 November 2023
Memperbarui kebijakan AWS terkelola	GuardDuty menambahkan izin baru, `organizations:ListAccounts` ke kebijakan AWS terkelola: AmazonGuardDutyFullAccess dan AmazonGuardDutyReadOnlyAccess.	16 November 2023

GuardDuty merilis jenis temuan baru yang menggunakan EKS Audit Log Monitoring.	EKS Audit Log Monitoring sekarang mendukung jenis temuan berikut di Asia Pasifik (Melbourne) (`ap-southeast-4`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	November 11, 2023

GuardDuty merilis jenis temuan baru yang menggunakan EKS Audit Log Monitoring.	EKS Audit Log Monitoring sekarang mendukung jenis temuan berikut di Asia Pasifik (Hyderabad) (`ap-south-2`), Eropa (Zurich) (`eu-central-2`), dan Eropa (Spanyol) () Wilayah. `eu-south-2` • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	10 November 2023

GuardDuty merilis jenis temuan baru yang menggunakan EKS Audit Log Monitoring.	EKS Audit Log Monitoring sekarang mendukung jenis temuan berikut. Jenis temuan ini belum tersedia di Asia Pasifik (Hyderabad) (`ap-south-2`), Eropa (Zurich) (), Eropa (Spanyol`eu-central-2`) (), dan Asia Pasifik (Melbourne`eu-south-2`) (). `ap-southeast-4` • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	8 November 2023

	• Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
EKS Runtime Monitoring merilis agen baru v1.3.1	EKS Runtime Monitoring merilis agen baru versi 1.3.1 yang mencakup tambalan dan pembaruan keamanan penting.	23 Oktober 2023
Atribut filter baru untuk menemukan	GuardDuty telah menambahkan kriteria baru untuk menyaring temuan yang dihasilkan. Akhiran domain permintaan DNS menyediakan domain tingkat kedua dan teratas yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.	17 Oktober 2023
EKS Runtime Monitoring merilis agen baru v1.3.0 yang mendukung Kubernetes versi 1.28	EKS Runtime Monitoring merilis agen baru versi 1.3.0 yang mendukung Kubernetes versi 1.28. Menambahkan dukungan untuk Ubuntu. Untuk informasi selengkapnya, lihat riwayat rilis agen add-on EKS.	5 Oktober 2023

Menambahkan jenis temuan berbasis S3 dan AWS CloudTrail machine learning (ML) ke Wilayah Asia Pasifik (Jakarta) dan Timur Tengah (UEA)	S3 berikut dan CloudTrail temuan yang mengidentifikasi perilaku anomali menggunak an model pembelajaran mesin deteksi anomali (ML) sekarang tersedia di Wilayah Asia Pasifik (Jakarta) dan Timur Tengah (UEA): GuardDuty • Discovery:S3/Anoma lousBehavior • Impact:S3/Anomalou sBehavior.Write • Impact:S3/Anomalou sBehavior.Delete • Impact:S3/Anomalou sBehavior.Permission • Exfiltration:S3/AnomalousBe havior • Exfiltration:IAMUser/Anomal ousBehavior • Impact:IAMUser/Ano malousBehavior • CredentialAccess:IAMUser/ AnomalousBehavior • DefenseEvasion:IAMUser/ AnomalousBehavior • InitialAccess:IAMUser/ AnomalousBehavior • Persistence:IAMUser/ AnomalousBehavior • PrivilegeEscalation:IAMUser /AnomalousBehavior	20 September 2023

	• Discovery:IAMUser/AnomalousBehavior	
GuardDuty EKS Runtime Monitoring memperkenalkan agen GuardDuty keamanan pengelola di tingkat cluster	EKS Runtime Monitoring menambahkan dukungan untuk mengelola agen GuardDuty keamanan untuk kluster EKS individu untuk memantau peristiwa runtime hanya dari cluster selektif ini. EKS Runtime Monitoring memperluas kemampuan ini dengan dukungan tag.	13 September 2023
GuardDuty Perlindungan Malware untuk EC2 memperluas dukungan ke lebih Wilayah AWS	Perlindungan Malware untuk EC2 sekarang tersedia di Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), Eropa (Zurich), dan Eropa (Spanyol).	11 September 2023

GuardDuty sekarang tersedia di Israel (Tel Aviv) Region	Menambahkan Wilayah Israel (Tel Aviv) ke daftar Wilayah AWS tempat sekarang GuardDuty tersedia. Rencana perlindungan berikut juga tersedia di Wilayah Israel (Tel Aviv): • Perlindungan EKSmencakup Pemantauan Log Audit EKS dan Pemantauan Runtime EKS. • Perlindungan Lambda. • Perlindungan Malware untuk EC2. • Perlindungan S3. Untuk informasi lebih lanjut tentang ketersediaan rencana perlindungan di Wilayah Israel (Tel Aviv), lihatWilayah dan titik akhir.	24 Agustus 2023
GuardDuty menambahkan konfigurasi aktifkan otomatis untuk organisasi Anda di tingkat rencana perlindungan	Perbarui konfigurasi organisasi untuk paket perlindungan di Wilayah Anda. Opsi konfigurasi yang memungkinkan adalah mengaktifkan semua akun, mengaktifkan otomatis untuk akun baru, atau tidak mengaktifkan otomatis untuk akun apa pun di organisasi Anda.	16 Agustus 2023

Jenis temuan S3 yang mengidentifikasi perilaku anomali menggunakan GuardDuty model pembelajaran mesin deteksi anomali (ML) sekarang tersedia di Asia Pasifik (Osaka)	Jenis temuan berikut sekarang tersedia di Wilayah Asia Pasifik (Osaka): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	10 Agustus 2023
EKS Runtime Monitoring sekarang tersedia di Asia Pasifik (Melbourne)	Pemantauan Runtime GuardDuty EKS dalam Perlindungan EKS menyediakan deteksi ancaman runtime untuk kluster Amazon EKS Anda di lingkungan. AWS Sekarang didukung di Wilayah Asia Pasifik (Melbourne).	8 Agustus 2023
Memperbarui daftar GuardDuty temuan yang memanggil pemindaian GuardDuty-initiated malware	Jenis temuan Pemantauan Runtime EKS tertentu sekarang dapat memanggil pemindaian GuardDuty-initiated malware di Anda. Akun AWS	Juli 19, 2023

GuardDuty mendukung 10.000 akun anggota melalui AWS Organizations	Akun GuardDuty administrator sekarang dapat mengelola maksimal 10.000 akun anggota melalui AWS Organizations. Ini juga termasuk maksimal 5000 akun anggota yang terkait dengan akun GuardDuty administrator melalui undangan.	29 Juni 2023
EKS Runtime Monitoring mengumumkan tiga jenis temuan baru.	EKS Runtime Monitoring mendukung tiga jenis temuan baru yang didasarkan pada teknik injeksi proses. Jenis temuan baru adalah DefenseEvasion:Runtime/ProcessInjection.Proc, DefenseEvasion:Runtime/ProcessInjection.Ptrace, dan DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite.	22 Juni 2023
EKS Runtime Monitoring merilis agen baru v1.2.0 yang mendukung Kubernetes versi 1.27	EKS Runtime Monitoring merilis agen baru versi 1.2.0 yang juga mendukung ARM64-based instance. Ditambahkan dukungan untuk Bottlerocket. Untuk informasi selengkapnya, lihat riwayat rilis agen add-on EKS.	Juni 16, 2023

GuardDuty konsol memberikan pandangan yang diringkas dari temuan Anda.	Dasbor ringkasan di GuardDuty konsol memberikan tampilan agregat GuardDuty temuan. Saat ini, dasbor menampilkan data melalui berbagai widget untuk 10.000 temuan terakhir yang dihasilkan untuk akun Anda (atau akun anggota jika Anda adalah akun GuardDuty administrator) untuk Wilayah saat ini.	12 Juni 2023
EKS Audit Log Monitoring sekarang tersedia di Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), Eropa (Zurich), dan Eropa (Spanyol)	Aktifkan Pemantauan Log Audit EKS (dalam Perlindungan EKS) untuk akun Anda untuk memantau log audit EKS dari kluster Amazon EKS Anda dan menganalisisnya untuk aktivitas yang berpotensi berbahaya dan mencurigakan.	1 Juni 2023
Pemantauan Log Audit EKS sekarang tersedia di Timur Tengah (UEA)	Pemantauan Log Audit EKS sekarang tersedia di Timur Tengah (UEA). Aktifkan Pemantauan Log Audit EKS untuk akun Anda untuk memantau log audit EKS dari kluster Amazon EKS Anda dan menganalisisnya untuk aktivitas yang berpotensi berbahaya dan mencurigakan.	3 Mei 2023

GuardDuty Perlindungan Malware untuk EC2 mengumumkan On-demand pemindaian malware	Perlindungan Malware untuk EC2 membantu Anda mendeteksi potensi keberadaan malware dalam volume Amazon EBS yang dilampirkan ke instans Amazon EC2 dan beban kerja kontainer Anda. Sekarang menawarkan dua jenis pemindaian — GuardDuty dimulai dan sesuai permintaan. GuardDuty-initiated Pemindaian malware memulai pemindaian tanpa agen dalam volume Amazon EBS secara otomatis hanya ketika GuardDuty menghasilkan salah satu Temuan yang memanggil pemindaian malware. GuardDuty-initiated Anda dapat memulai pemindaian On-demand malware untuk instans Amazon EC2 di akun Anda dengan memberikan Nama Sumber Daya Amazon (ARN) yang terkait dengan instans Amazon EC2 tersebut. Untuk informasi selengkapnya tentang perbedaan kedua jenis pemindaian, lihat Perlindungan Malware untuk EC2. • GuardDuty-initiated pemindaian malware • On-demand pemindaian malware	27 April 2023

GuardDuty mengumumkan Perlindungan Lambda	Perlindungan Lambda membantu Anda mengident ifikasi potensi ancaman keamanan dalam fungsi Anda AWS Lambda . • Jenis temuan Perlindungan Lambda • Memperbaiki fungsi Lambda yang berpotensi dikomprom ikan	20 April 2023
GuardDuty sekarang tersedia di Wilayah Asia Pasifik (Melbourne)	Menambahkan Asia Pasifik (Melbourne) ke daftar Wilayah AWS tempat GuardDuty tersedia. Untuk informasi tentang fitur yang tersedia di Wilayah ini, lihat Wilayah dan titik akhir.	19 April 2023
GuardDuty menambahkan 3 jenis temuan EC2 baru	GuardDuty memperkenalkan jenis temuan baru untuk mendeteksi penggunaan resolver DNS eksternal dan teknologi DNS terenkrip si. Untuk informasi tentang Wilayah AWS di mana jenis temuan ini didukung, lihat Wilayah dan titik akhir. • DefenseEvasion:EC2/ UnusualDNSResolver • DefenseEvasion:EC2/ UnusualDoHActivity • DefenseEvasion:EC2/ UnusualDoTActivity	5 April 2023

GuardDuty mengumumkan Pemantauan Runtime EKS di Perlindungan EKS	Pemantauan Runtime EKS dalam Perlindungan EKS menyediakan deteksi ancaman runtime untuk kluster Amazon EKS Anda di lingkungan. AWS Ini menggunakan agen add-on Amazon EKS (`aws-guardduty-agent`) yang mengumpulkan peristiwa Runtime dari beban kerja EKS Anda. Setelah GuardDuty menerima peristiwa runtime ini, ia memantau dan menganalisisnya untuk mengidentifikasi potensi ancaman keamanan yang mencurigakan. Untuk informasi selengkapnya, lihat Menemukan detail dan jenis pencarian Pemantauan Waktu Jalan EKS.	30 Maret 2023

GuardDuty menambahkan fungsionalitas baru - `autoEnableOrganizationMembers`	Amazon GuardDuty menambahkan opsi konfigurasi organisasi baru yang membantu akun GuardDuty administrator mengaudit dan menegakkan (jika diperlukan) yang GuardDuty diaktifkan untuk `ALL` anggota organisasi mereka. Praktik terbaik sekarang adalah menggunakan `autoEnableOrganizationMembers` alih-alih `autoEnable` . `autoEnable` sudah usang tetapi masih didukung. API berikut dipengaruhi oleh fungsionalitas baru ini: • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	Maret 23, 2023

Fitur Perlindungan RDS di Amazon sekarang GuardDuty tersedia secara umum	GuardDuty Perlindungan RDS memantau dan memprofil kan aktivitas login RDS untuk mengidentifikasi perilaku login yang mencurigakan pada instans database Amazon Aurora Anda. Untuk informasi tentang yang Wilayah AWS mendukung Perlindungan RDS, lihat Wilayah dan titik akhir.	16 Maret 2023
GuardDuty mengumumkan aktivasi fitur	Secara historis, GuardDuty API mengizinkan konfigura si fitur dan sumber data, tetapi sekarang, semua jenis GuardDuty perlindungan baru akan dikonfigurasi sebagai fitur dan bukan sebagai sumber data. GuardDuty masih mendukung sumber data melalui API tetapi tidak akan menambahk an API baru. Aktivasi fitur memengaruhi perilaku API yang digunakan untuk mengaktifkan GuardDuty atau jenis perlindungan di dalamnya GuardDuty. Jika Anda mengelola GuardDuty akun Anda melalui template API, SDK, atau CFN, lihat perubahan GuardDuty API pada Maret 2023.	16 Maret 2023

GuardDuty Perlindungan Malware untuk EC2 sekarang tersedia di Wilayah Timur Tengah (UEA)	Fitur Perlindungan Malware untuk EC2 di GuardDuty didukung di Wilayah Timur Tengah (UEA). Untuk informasi selengkapnya, lihat Wilayah dan titik akhir.	13 Maret 2023
Amazon GuardDuty telah memperbarui Service-linked peran (SLR)	GuardDuty menambahkan izin baru berikut untuk mendukung fitur GuardDuty EKS Runtime Monitoring yang akan datang. • Gunakan tindakan Amazon EKS untuk mengelola dan mengambil informasi tentang kluster EKS, dan mengelola add-on EKS di kluster EKS. Tindakan EKS juga mengambil informasi tentang tag yang terkait dengan GuardDuty. `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	8 Maret 2023
Amazon GuardDuty telah memperbarui Service-linked peran (SLR)	GuardDuty SLR telah diperbarui untuk memungkinkan pembuatan Perlindungan Malware untuk EC2 SLR setelah Perlindungan Malware untuk EC2 diaktifkan.	21 Februari 2023

GuardDuty membutuhkan TLS v1.2 atau yang lebih baru	Untuk berkomunikasi dengan AWS sumber daya, GuardDuty membutuhkan dan mendukung TLS v1.2 atau yang lebih baru. Untuk informasi selengkapnya, lihat Perlindungan data dan Keamanan infrastruktur.	14 Februari 2023
GuardDuty sekarang tersedia di Wilayah Asia Pasifik (Hyderabad)	Menambahkan Wilayah Asia Pasifik (Hyderabad) ke daftar Wilayah AWS tempat GuardDuty tersedia. Untuk informasi selengkapnya, lihat Wilayah dan titik akhir.	14 Februari 2023
Panduan GuardDuty Pengguna Amazon selaras dengan praktik terbaik IAM	Memperbarui panduan untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi lebih lanjut, lihat Praktik terbaik keamanan di IAM.	Februari 10, 2023
GuardDuty sekarang tersedia di Wilayah Eropa (Spanyol)	Menambahkan Eropa (Spanyol) ke Wilayah AWS daftar GuardDuty di mana tersedia. Untuk informasi selengkapnya, lihat Wilayah dan titik akhir.	Februari 8, 2023
GuardDuty sekarang tersedia di Wilayah Eropa (Zurich)	Menambahkan Eropa (Zurich) ke daftar Wilayah AWS di mana GuardDuty tersedia. Untuk informasi selengkapnya, lihat Wilayah dan titik akhir.	12 Desember 2022

Pratinjau rilis fitur baru - Perlindungan GuardDuty RDS	GuardDuty Perlindungan RDS memantau dan memprofil kan aktivitas login RDS untuk mengidentifikasi perilaku login yang mencurigakan pada instans database Amazon Aurora Anda. Saat ini, tersedia untuk rilis pratinjau dalam lima Wilayah AWS. Untuk informasi selengkapnya, lihat Wilayah dan titik akhir.	30 November 2022
GuardDuty sekarang tersedia di Wilayah Timur Tengah (UEA)	Menambahkan Timur Tengah (UEA) ke daftar Wilayah AWS di mana GuardDuty tersedia. Untuk informasi selengkapnya, lihat Wilayah dan titik akhir.	6 Oktober 2022

Menambahkan konten untuk fitur baru - Perlindungan GuardDuty Malware untuk EC2	GuardDuty Perlindungan Malware untuk EC2 adalah peningkatan opsional untuk Amazon. GuardDuty Sementara GuardDuty mengidentifikasi sumber daya yang berisiko, Perlindungan Malware untuk EC2 mendeteksi malware yang mungkin menjadi sumber kompromi. Dengan Perlindungan Malware untuk EC2 diaktifkan, setiap kali GuardDuty mendeteksi perilaku mencurigakan pada instans Amazon EC2 atau beban kerja kontainer yang menunjukkan GuardDuty malware, Perlindungan Malware untuk EC2 memulai pemindaian tanpa agen pada volume EBS yang dilampirkan ke instans EC2 yang terkena dampak atau beban kerja kontainer untuk mendeteksi keberadaan malware. Untuk informasi tentang cara kerja Perlindungan Malware untuk EC2 dan mengonfigurasi fitur ini, lihat Perlindungan GuardDuty Malware untuk EC2. • Untuk informasi tentang Perlindungan Malware	26 Juli 2022

	untuk temuan EC2, lihat Menemukan detail. • Untuk informasi tentang memulihkan instans EC2 yang dikompromikan dan wadah mandiri, lihat Memperbaiki masalah keamanan yang ditemukan oleh. GuardDuty • Untuk informasi tentang mengaudit CloudWatch log untuk pemindaian malware dan alasan melewatkan sumber daya selama pemindaian malware, lihat Memahami CloudWatch Log dan lewati alasannya. • Untuk informasi tentang deteksi ancaman positif palsu, lihat Melaporkan positif palsu di Perlindungan GuardDuty Malware untuk EC2.	
Pensiunan satu jenis temuan	Exfiltration:S3/ObjectRead.Unusualtelah pensiun.	Juli 5, 2022

Menambahkan jenis temuan S3 baru yang mengidentifikasi perilaku anomali menggunakan GuardDuty model pembelajaran mesin deteksi anomali (ML).	Menambahkan jenis temuan S3 baru berikut. Jenis temuan ini mengidentifikasi apakah permintaan API memanggil entitas IAM dengan cara yang anomali. Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa beranomali yang terkait dengan teknik yang digunakan oleh penyerang . Untuk mempelajari lebih lanjut tentang masing-masing temuan baru ini, lihat tipe temuan S3. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	Juli 5, 2022

Ditambahkan konten GuardDuty EKS Protection untuk GuardDuty	GuardDuty sekarang dapat menghasilkan temuan untuk sumber daya Amazon EKS Anda melalui pemantauan log audit EKS. Untuk mempelajari cara mengonfigurasi fitur ini, lihat Perlindungan EKS di Amazon GuardDuty. Untuk daftar temuan yang GuardDuty dapat dihasilkan untuk sumber daya Amazon EKS, lihat temuan Kubernetes. Panduan remediasi baru telah ditambahkan untuk mendukung remediasi temuan ini dalam panduan remediasi temuan Kubernetes.	Januari 25, 2022
Ditambahkan 1 temuan baru	Temuan baru UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS telah ditambahkan. Temuan ini memberi tahu Anda kapan kredensyal instans Anda diakses oleh AWS akun di luar lingkungan Anda. AWS	20 Januari 2022

Memperbarui jenis temuan untuk membantu mengidentifikasi masalah yang terkait dengan log4j	Amazon GuardDuty telah memperbarui jenis temuan berikut untuk membantu mengidentifikasi dan memprioritaskan masalah yang terkait dengan CVE-2021-44228 dan CVE-2021-45046:Backdoor:EC2/C&CActivity.B;;Backdoor:EC2/C&CActivity.B!DNS. Behavior:EC2/NetworkPortUnusual	Desember 22, 2021
Menemukan Perubahan	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltrationtelah diubah menjadiUnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. Versi temuan yang disempurnakan ini mempelajari lokasi khas yang digunakan kredensil Anda untuk mengurangi temuan dari lalu lintas yang diarahkan melalui jaringan premis. UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	7 September 2021
Perbarui ke GuardDuty SLR	GuardDuty SLR telah diperbarui dengan tindakan baru untuk meningkatkan akurasi pencarian.	Agustus 3, 2021

Menambahkan informasi sumber data untuk setiap jenis temuan.	Menemukan deskripsi sekarang berisi informasi tentang sumber data yang GuardDuty digunakan untuk menghasilkan temuan itu.	10 Mei 2021
Pensiunan 13 jenis pencarian.	13 temuan telah pensiun untuk diganti dengan Anomalous Behavoir temuan baru. Persistence:IAMUser/NetworkPermissions, Persistence:IAMUser/ResourcePermissions, Persistence:IAMUser/UserPermissions, PrivilegeEscalation:IAMUser/AdministrativePermissions, Recon:IAMUser/NetworkPermissions, Recon:IAMUser/ResourcePermissions, Recon:IAMUser/UserPermissions,, ResourceConsumption:IAMUser/ComputeResources, Stealth:IAMUser/LoggingConfigurationModified, Discovery:S3/BucketEnumeration.Unusual, Impact:S3/ObjectDelete.Unusual, Impact:S3/PermissionsModification.Unusual, dan UnauthorizedAccess:IAMUser/ConsoleLogin.	12 Maret 2021

Menambahkan 8 jenis temuan baru untuk perilaku anomali.	Menambahkan 8 jenis IAMUser temuan baru berdasarkan perilaku anomali untuk kepala sekolah IAM. CredentialAccess:IAMUser/AnomalousBehavior, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehavior, Impact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior, Persistence:IAMUser/AnomalousBehavior, PrivilegeEscalation:IAMUser/AnomalousBehavior.	12 Maret 2021
Menambahkan temuan EC2 berdasarkan reputasi domain.	Menambahkan 4 tipe temuan Impact yang baru berdasarkan reputasi domain. Impact:EC2/AbusedDomainRequest.Reputation , Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation. Juga menambahkan temuan EC2 baru untuk C&cActivity. Impact:EC2/SuspiciousDomainRequest.Reputation	27 Januari 2021

Ditambahkan 4 jenis temuan baru.	Menambahkan 3 temuan S3 MaliciousIPCaller yang baru. Discovery:S3/MaliciousIPCaller, Exfiltration:S3/MaliciousIPCaller, Impact:S3/MaliciousIPCaller. Juga menambahkan temuan EC2 baru untuk C&cActivity. Backdoor:EC2/C&CActivity.B	21 Desember 2020
Pensiun tipe UnauthorizedAccess:EC2/TorIPCaller temuan.	Jenis UnauthorizedAccess:EC2/TorIPCaller temuan sekarang sudah pensiun dari GuardDuty. Pelajari selengkapnya.	1 Oktober 2020
Menambahkan jenis Impact:EC2/WinRmBruteForce temuan.	Menambahkan temuan Dampak baru,Impact:EC2/WinRmBruteForce. Pelajari selengkapnya.	17 September 2020
Menambahkan jenis Impact:EC2/PortSweep temuan.	Menambahkan temuan Dampak baru,Impact:EC2/PortSweep. Pelajari selengkapnya.	17 September 2020
GuardDuty sekarang tersedia di Wilayah Afrika (Cape Town) dan Eropa (Milan).	Menambahkan Afrika (Cape Town) dan Eropa (Milan) ke daftar AWS Wilayah di mana GuardDuty tersedia. Pelajari selengkapnya	31 Juli 2020

Menambahkan detail penggunaan baru untuk memantau GuardDuty biaya.	Sekarang Anda dapat menggunakan metrik baru untuk menanyakan data biaya GuardDuty penggunaan untuk akun dan akun yang Anda kelola. Gambaran umum baru tentang biaya penggunaan tersedia di konsol di https://console.aws.amazon.com/guardduty/. Informasi selengkapnya dapat diakses melalui API.	31 Juli 2020
Menambahkan konten yang mencakup perlindungan S3 melalui pemantauan peristiwa data S3 di. GuardDuty	GuardDuty S3 Protection sekarang tersedia melalui pemantauan peristiwa pesawat data S3 sebagai sumber data baru. Akun baru akan mengaktifkan fitur ini secara otomatis. Jika Anda sudah menggunakan, GuardDuty Anda dapat mengaktifkan sumber data baru untuk diri sendiri atau akun anggota Anda.	31 Juli 2020
Menambahkan 14 Temuan S3 baru.	14 tipe temuan S3 yang baru telah ditambahkan untuk bidang kendali S3 dan sumber bidang data.	31 Juli 2020

Menambahkan dukungan tambahan untuk temuan S3 dan mengubah 2 nama tipe temuan yang ada.	GuardDuty temuan sekarang mencakup rincian lebih lanjut untuk temuan yang melibatkan ember S3. Jenis temuan yang ada yang terkait dengan aktivitas S3 telah diganti namanya: Policy:IAMUser/S3BlockPublicAccessDisabled telah diubah menjadi. Policy:S3/BucketBlockPublicAccessDisabled Stealth:IAMUser/S3ServerAccessLoggingDisabledtelah diubah menjadiStealth:S3/ServerAccessLoggingDisabled.	28 Mei 2020
Menambahkan konten untuk AWS Organizations integrasi.	GuardDuty sekarang terintegrasi dengan administrator AWS Organizations yang didelegasikan untuk memungkinkan Anda mengelola GuardDuty akun dalam organisasi Anda. Ketika Anda menetapkan administrator yang didelegasikan sebagai akun GuardDuty administrator, Anda dapat secara otomatis mengaktifkan GuardDuty anggota organisasi mana pun yang akan dikelola oleh akun administrator yang didelegasikan. Anda juga dapat mengaktifkan secara otomatis GuardDuty di akun AWS Organizations anggota baru. Pelajari selengkapnya.	20 April 2020

Menambahkan konten untuk fitur temuan ekspor.	Menambahkan konten yang menjelaskan fitur Temuan Ekspor dari GuardDuty.	14 November 2019
Menambahkan jenis UnauthorizedAccess:EC2/MetadataDNSRebind temuan.	Menambahkan temuan Tidak Sah baru,UnauthorizedAccess:EC2/MetadataDNSRebind. Pelajari selengkapnya.	10 Oktober 2019
Menambahkan jenis Stealth:IAMUser/S3ServerAccessLoggingDisabled temuan.	Menambahkan temuan Stealth baru,Stealth:IAMUser/S3ServerAccessLoggingDisabled. Pelajari selengkapnya.	10 Oktober 2019
Menambahkan jenis Policy:IAMUser/S3BlockPublicAccessDisabled temuan.	Menambahkan temuan Kebijakan baru,Policy:IAMUser/S3BlockPublicAccessDisabled. Pelajari selengkapnya.	10 Oktober 2019
Pensiun tipe Backdoor:EC2/XORDDOS temuan.	Jenis Backdoor:EC2/XORDDOS temuan sekarang sudah pensiun dari GuardDuty. Pelajari lebih lanjut	12 Juni 2019
Menambahkan jenis Privilege Escalation temuan.	Jenis PrivilegeEscalation temuan mendeteksi ketika pengguna mencoba untuk menetapkan hak istimewa yang meningkat dan lebih permisif ke akun mereka. Pelajari selengkapnya	14 Mei 2019
GuardDuty sekarang tersedia di Wilayah Eropa (Stockholm).	Menambahkan Europe (Stockholm) ke daftar AWS Wilayah di mana GuardDuty tersedia. Pelajari selengkapnya	9 Mei 2019

Menambahkan jenis temuan baru,Recon:EC2/PortProbeEMRUnprotectedPort.	Temuan ini memberi tahu Anda bahwa port EMR-related sensitif pada Instans EC2 tidak diblokir dan sedang diselidiki secara aktif. Pelajari selengkapnya	8 Mei 2019
Menambahkan 5 jenis temuan baru yang mendeteksi jika instans EC2 Anda berpotensi digunakan untuk serangan denial of service (DoS).	Temuan ini menginformasikan bahwa instans EC2 di lingkungan Anda yang berperilaku dengan cara yang mungkin mengindikasikan bahwa instans sedang digunakan untuk melakukan serangan Denial of Service (DoS). Pelajari selengkapnya	8 Maret 2019
Menambahkan jenis temuan baru: Policy:IAMUser/RootCredentialUsage	Policy:IAMUser/RootCredentialUsagejenis pencarian memberi tahu Anda bahwa kredensi masuk pengguna root Anda Akun AWS sedang digunakan untuk membuat permintaan terprogram ke layanan. AWS Pelajari selengkapnya	24 Januari 2019

UnauthorizedAccess:IAMUser/UnusualASNCallertipe temuan telah pensiun	Jenis UnauthorizedAccess :IAMUser/UnusualASNCaller temuan telah pensiun. Anda sekarang akan diberi tahu tentang aktivitas yang dipanggil dari jaringan yang tidak biasa melalui jenis GuardDuty temuan aktif lainnya. Tipe temuan yang dihasilkan akan didasarka n pada kategori API yang dipanggil dari jaringan yang tidak biasa. Pelajari selengkap nya	21 Desember 2018
Menambahkan dua jenis temuan baru: PenTest:I AMUser/ParrotLinux dan PenTest:IAMUser/PentooLinux	PenTest:IAMUser/ParrotLinux jenis pencarian memberi tahu Anda bahwa komputer yang menjalankan Parrot Security Linux melakukan panggilan API menggunak an kredensil milik akun Anda. AWS PenTest:IAMUser/Pe ntooLinuxjenis pencarian memberi tahu Anda bahwa mesin yang menjalankan Pentoo Linux melakukan panggilan API menggunak an kredensil milik akun Anda. AWS Pelajari selengkapnya	21 Desember 2018

Menambahkan dukungan untuk topik SNS GuardDuty pengumuman Amazon	Anda sekarang dapat berlangganan topik SNS GuardDuty pengumuman untuk menerima pemberita huan tentang jenis temuan yang baru dirilis, pembaruan untuk jenis temuan yang ada, dan perubahan fungsionalitas lainnya. Notifikasi tersedia dalam semua format yang didukung Amazon SNS. Pelajari selengkapnya	21 November 2018
Menambahkan dua jenis temuan baru: UnauthorizedAccess:EC2/TorClient dan UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClienttipe pencarian memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda membuat koneksi ke Tor Guard atau node Authority. UnauthorizedAccess:EC2/TorRelayjenis pencarian memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda membuat koneksi ke jaringan Tor dengan cara yang menunjukkan bahwa itu bertindak sebagai relai Tor. Pelajari selengkapnya	16 Novbucket 2018

Menambahkan jenis temuan baru: CryptoCurrency:EC2/BitcoinTool.B	Temuan ini memberi tahu Anda bahwa instans EC2 di AWS lingkungan Anda menanyakan nama domain yang terkait dengan Bitcoin, atau aktivitas terkait cryptocurrency lainnya. Pelajari selengkapnya	9 November 2018
Menambahkan dukungan untuk memperbarui frekuensi pemberitahuan yang dikirim ke CloudWatch Acara	Anda sekarang dapat memperbarui frekuensi pemberitahuan yang dikirim ke CloudWatch Acara untuk kejadian berikutnya dari temuan yang ada. Nilai yang mungkin adalah 15 menit, 1 jam, atau default 6 jam. Pelajari selengkapnya	9 Oktober 2018
Ditambahkan dukungan Wilayah	Menambahkan dukungan Wilayah untuk AWS GovCloud (US-West) Pelajari lebih lanjut	25 Juli 2018
Ditambahkan dukungan untuk CloudFormation StackSets di GuardDuty	Anda dapat menggunakan GuardDuty template Aktifkan Amazon untuk mengaktifkan GuardDuty secara bersamaan di beberapa akun. Pelajari selengkapnya	25 Juni 2018

Menambahkan dukungan untuk aturan GuardDuty arsip otomatis	Pelanggan kini dapat membuat aturan pengarsip an otomatis granular untuk penekanan temuan. Untuk temuan yang cocok dengan aturan arsip otomatis, tandai GuardDuty secara otomatis sebagai diarsipkan. Hal ini memungkinkan pelanggan untuk lebih menyesuaikan GuardDuty untuk menyimpan hanya temuan yang relevan dalam tabel temuan saat ini. Pelajari selengkapnya	4 Mei 2018
GuardDuty tersedia di Wilayah Eropa (Paris)	GuardDuty sekarang tersedia di Eropa (Paris), memungkin kan Anda untuk memperlua s pemantauan keamanan berkelanjutan dan deteksi ancaman di Wilayah ini. Pelajari selengkapnya	29 Maret 2018
Membuat akun GuardDuty administrator dan akun anggota CloudFormation sekarang didukung.	Untuk informasi selengkapnya, lihat `AWS::GuardDuty::master` dan `AWS::GuardDuty::member`.	6 Maret 2018
Menambahkan sembilan deteksi CloudTrail-based anomali baru.	Jenis temuan baru ini diaktifka n secara otomatis GuardDuty di semua Wilayah yang didukung. Pelajari selengkap nya	28 Februari 2018

Menambahkan tiga deteksi intelijen ancaman baru (tipe pencarian).	Jenis temuan baru ini diaktifkan secara otomatis GuardDuty di semua Wilayah yang didukung. Pelajari lebih lanjut	5 Februari 2018
Batasi kenaikan untuk akun GuardDuty anggota.	Dengan rilis ini, Anda dapat memiliki hingga 1000 akun GuardDuty anggota ditambahkan per AWS akun (akun akun GuardDuty administrator). Pelajari selengkapnya	25 Januari 2018
Perubahan dalam unggahan dan pengelolaan lebih lanjut dari daftar IP tepercaya dan daftar ancaman untuk akun GuardDuty administrator dan akun anggota.	Dengan rilis ini, Pengguna dari akun GuardDuty akun administrator dapat mengunggah dan mengelola daftar IP tepercaya dan daftar ancaman. Pengguna dari GuardDuty akun anggota tidak dapat mengunggah dan mengelola daftar. Daftar IP tepercaya dan daftar ancaman yang diunggah oleh akun akun administrator dikenakan pada GuardDuty fungsionalitas di akun anggotanya. Pelajari selengkapnya	25 Januari 2018

Pembaruan lebih awal

Perubahan	Deskripsi	Date
Publikasi awal	Publikasi awal Panduan GuardDuty Pengguna Amazon.	28 November 2017

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.